Same-site Proactive BrowsingInstance Swap Changes

rakina@chromium.org, …
Last updated: 2020/05

See arthursonzogni@'s original doc for background information and launch plan doc (google-internal).

What's changing?
- We will swap BrowsingInstances on most main-frame navigations, both same-site and cross-site.
    - Exceptions: Same-document navigations, pages with >1 active related contents, reload, same-page navigations, other types of navigation that won't create a new history entry, etc.
- Note: This feature is needed for BFCache, and will only be enabled when BFCache is enabled. The cross-site-only version of proactive BrowsingInstance swap is already implemented and enabled for BFCache.

Permanent behavior changes
- On most main-frame navigations the BrowsingInstance, SiteInstance, RenderFrameHost, RenderViewHost, Page, etc. will change. However, when we can, we will reuse the previous page's process.
- Cancellation of previous navigations when there are multiple pending navigations - see https://groups.google.com/a/chromium.org/g/navigation-dev/c/Y2jpfDl8k_8/m/zgHPgTF8AwAJ
    - Previously if there are two ongoing navigations, where one is same-site and the other is cross-site, both of them will not get canceled until either one of them commits.
    - Now when there's a same-site nav and cross-site nav (both haven't committed) it's possible for them to both be cross-RFH, so the last navigation will win (previous navigations will get canceled).
- Scripting relationships might get dropped on history navigations.
    - Example: crbug.com/1043162. We navigate from A1->A2, then A2 opens a popup B, and we navigate back to A1.
        - Previously: A1 and A2 will be in the same BI, A2 will be able to script B.
        - With Proactive BI swap: A1 and A2 might be in a different BIs, in which case A won't be able to script B2.
    - See thread and doc about spec changes.

- ○ Note that this only happens on history navigations, as we won't proactively swap BIs on a normal navigation when the current page has active scripting relationships (active related contents > 1).

TODOs / currently broken, will be fixed
- ● Unload handler timing
  - ○ See doc: [Unload- & freeze-time events & same-site RFH swap](#)
- ● Layout test failures
  - ○ A lot of navigation-related layout tests are timing out/failing because the TestRunner does not expect an RFH change on same-site navigation - this is being investigated and will be fixed soon!
  - ○ Some other tests are working correctly but dumps a list of navigation events that look different with proactive BI swap because we're creating more speculative RenderFrameHosts. These can be fixed with virtual TestExpectations, however we need to set params for SameSite ProactivelySwapBrowsingInstance, which is not currently supported (see [bug](#)).
  - ○ All the failing layout tests are currently tracked here [[link](#)]
- ● MediaHistoryBrowserTest
  - ○ [Additional playbacks recorded with the patch](#) - but this might not be a Proactive BI Swap bug? When the navigation in the test is changed from same-site to cross-site [[CL](#)], additional playbacks still gets recorded even without the Proactive BI Swap patch (currently asking media people)

FIXED
- ● Carrying over WebPreferences on same-site navigations
  - ○ [WebPreferences](#) are per-RenderView and gets reset on BI swap because we change RenderViews. However, some (or all?) of them needs to be retained for a specific site (example: [javascript_enabled](#))
  - ○ **Solution**: We should change the code to copy the WebPreferences when we are doing a RVH swap on same-site navigation (maybe during ReadyToCommitNavigation so we can access both the old and new RVH?). We need to know that we are doing a proactive BI swap too (or maybe just check if it's same-site?)
- ● Process reuse on history navigation
  - ○ Scenario: Going from a.com/foo -> a.com/bar, we swap BIs but reuse the process. When we do a history navigation from a.com/bar to a.com/foo, we will swap BIs but we won't reuse the process again (because the history navigation code does not know that it was a proactive BI swap, it only sees that the BIs are different).
  - ○ **Solution**: add whether we proactive swapped or not to navigation entries?