Make ArrayBufferAllocator Isolate-independent

(externally visible, non-confidential)

Author: ahaas@
Status: Draft | Final
Tracking Bug: https://crbug.com/1008840
Created: 2019-10-07 / **Updated:** 2019-10-07

Motivation

We are working on moving ArrayBuffer backing store memory ownership to V8's `v8::BackingStore` class, see tracking bug https://crbug.com/v8/9380.
One problem there is that some `ArrayBuffer` backing stores are allocated by the embedder without using the V8 isolate. Creating `v8::BackingStore` objects, however, require the isolate at the moment, because the `ArrayBufferAllocator` is stored in the isolate. Therefore we want to make the `ArrayBufferAllocator` isolate-independent by moving it to the `v8::Platform` so that we can move all allocator of `ArrayBuffer` backing stores to V8.

Proposed changes

1. Introduce new getter to `v8::Platform` for the `ArrayBufferAllocator`, with a default implementation which returns `nullptr`.
2. In `Isolate::Initialize(CreateParams& params)`, if `v8::Platform::GetArrayBufferAllocator` returns an allocator, store that allocator in the isolate instead of the allocator passed by `params`. Additionally we check that any embedder who provides an ArrayBufferAllocator to the `v8::Platform` does not pass an `ArrayBufferAllocator` to `Isolate::Initialization(CreateParams& params)`. Thereby we make sure that `ArrayBufferAllocators` are not mixed up.
3. Change embedders to provide the `ArrayBufferAllocator` through the `v8::Platform`.

Risks

There may be a reason why the `ArrayBufferAllocator` is isolate-specific. There may be cases where different isolates have different `ArrayBufferAllocators` at the same time.

However, we are not aware of such cases. It is even not clear if having different `ArrayBufferAllocators` would even work at the moment