MODULE *Cloudformation*

CloudFormation an *AWS* service that provisions *AWS* cloud infrastructure. Infrastructure is provisioned in related groupings called "stacks." These stacks can be in one of several states. This spec verifies that all state transitions are accounted for and that no deadlock (a state that has no further possible action) can occur.

CONSTANTS *CREATE_COMPLETE*,
CREATE_IN_PROGRESS,
CREATE_FAILED,
DELETE_COMPLETE,
DELETE_FAILED,
DELETE_IN_PROGRESS,
REVIEW_IN_PROGRESS,
ROLLBACK_COMPLETE,
ROLLBACK_FAILED,
ROLLBACK_IN_PROGRESS,
UPDATE_COMPLETE,
UPDATE_COMPLETE_CLEANUP_IN_PROGRESS,
UPDATE_IN_PROGRESS,
UPDATE_ROLLBACK_COMPLETE,
UPDATE_ROLLBACK_COMPLETE_CLEANUP_IN_PROGRESS,
UPDATE_ROLLBACK_FAILED,
UPDATE_ROLLBACK_IN_PROGRESS

VARIABLES *status*

$vars \triangleq \langle status \rangle$

$TypeInvariant \triangleq status \in \{$
CREATE_COMPLETE,
CREATE_IN_PROGRESS,
CREATE_FAILED,
DELETE_COMPLETE,
DELETE_FAILED,
DELETE_IN_PROGRESS,
REVIEW_IN_PROGRESS,
ROLLBACK_COMPLETE,
ROLLBACK_FAILED,
ROLLBACK_IN_PROGRESS,
UPDATE_COMPLETE,
UPDATE_COMPLETE_CLEANUP_IN_PROGRESS,
UPDATE_IN_PROGRESS,
UPDATE_ROLLBACK_COMPLETE,
UPDATE_ROLLBACK_COMPLETE_CLEANUP_IN_PROGRESS,
UPDATE_ROLLBACK_FAILED,
UPDATE_ROLLBACK_IN_PROGRESS,

"default"
}

$Init \triangleq status =$ "default"
$DoesNotExist(s) \triangleq s =$ "default"
$IsCompleted(s) \triangleq s \in \{CREATE\_COMPLETE, DELETE\_COMPLETE, ROLLBACK\_COMPLETE, UPL$
$IsFailed(s) \triangleq s \in \{CREATE\_FAILED, DELETE\_FAILED, ROLLBACK\_FAILED, UPDATE\_ROLLBACI$

Ongoing creation of one or more stacks.

$$CreateInProgress \triangleq \land DoesNotExist(status) \land status' = CREATE\_IN\_PROGRESS$$

Successful creation of one or more stacks.

$$CreateComplete \triangleq \land status = CREATE\_IN\_PROGRESS \land status' = CREATE\_COMPLETE$$

Unsuccessful creation of one or more stacks. View the stack events to see any associated error messages. Possible reasons for a failed creation include insufficient permissions to work with all resources in the stack, parameter values rejected by an *AWS* service, or a timeout during resource creation.

$$CreateFailed \triangleq \land status = CREATE\_IN\_PROGRESS \land status' = CREATE\_FAILED$$

Ongoing removal of one or more stacks.

$$DeleteInProgress \triangleq \land IsCompleted(status) \lor IsFailed(status) \land status' = DELETE\_IN\_PROGRESS$$

Successful deletion of one or more stacks. Deleted stacks are retained and viewable for 90 days.

$$DeleteComplete \triangleq \land status = DELETE\_IN\_PROGRESS \land status' = DELETE\_COMPLETE$$

Unsuccessful deletion of one or more stacks. Because the delete failed, you might have some resources that are still running; however, you cannot work with or update the stack. Delete the stack again or view the stack events to see any associated error messages.

$$DeleteFailed \triangleq \land status = DELETE\_IN\_PROGRESS \land status' = DELETE\_FAILED$$

Ongoing update of one or more stacks.

$$UpdateInProgress \triangleq \land IsCompleted(status) \land status' = UPDATE\_IN\_PROGRESS$$

Successful update of one or more stacks.

$$UpdateComplete \triangleq \land status = UPDATE\_IN\_PROGRESS \lor status = UPDATE\_COMPLETE\_CLEANUP\_IN\_PROGRESS \land status' = UPDATE\_COMPLETE$$

Ongoing removal of old resources for one or more stacks after a successful stack update. For stack updates that require resources to be replaced, *AWS CloudFormation* creates the new resources first and then deletes the old resources to help reduce any interruptions with your stack. In this state, the stack has been updated and is usable, but *AWS CloudFormation* is still deleting the old resources.

$$UpdateCompleteCleanupInProgress \triangleq \land status = UPDATE\_IN\_PROGRESS \land status' = UPDATE\_COMPLETE\_CLEANUP\_IN\_PROGRESS$$

Ongoing removal of one or more stacks after a failed stack creation or after an explicitly cancelled stack creation.

$$RollbackInProgress \triangleq \land status = CREATE\_IN\_PROGRESS \land status' = ROLLBACK\_IN\_PROGRESS$$

Successful removal of one or more stacks after a failed stack creation or after an explicitly canceled stack creation. Any resources that were created during the create stack action are deleted.

This status exists only after a failed stack creation. It signifies that all operations from the partially created stack have been appropriately cleaned up. When in this state, only a delete operation can be performed.

$$RollbackComplete \triangleq \land status = ROLLBACK\_IN\_PROGRESS \land status' = ROLLBACK\_COMPLETE$$

Unsuccessful removal of one or more stacks after a failed stack creation or after an explicitly canceled stack creation. Delete the stack or view the stack events to see any associated error messages.

$$RollbackFailed \triangleq \land status = ROLLBACK\_IN\_PROGRESS \land status' = ROLLBACK\_FAILED$$

Ongoing return of one or more stacks to the previous working state after failed stack update.

$$UpdateRollbackInProgress \triangleq \land status = UPDATE\_IN\_PROGRESS \land status' = UPDATE\_ROLLBACK\_IN\_PROGRESS$$

Successful return of one or more stacks to a previous working state after a failed stack update.

$$UpdateRollbackComplete \triangleq \land status = UPDATE\_ROLLBACK\_IN\_PROGRESS \lor status = UPDATE\_ROLLBACK\_COMPLETE\_CLEANUP\_IN\_PROGRES \land status' = UPDATE\_ROLLBACK\_COMPLETE$$

Unsuccessful return of one or more stacks to a previous working state after a failed stack update. When in this state, you can delete the stack or continue rollback. You might need to fix errors before your stack can return to a working state. Or, you can contact customer support to restore the stack to a usable state.

$$UpdateRollbackFailed \triangleq \land status = UPDATE\_ROLLBACK\_IN\_PROGRESS \land status' = UPDATE\_ROLLBACK\_FAILED$$

This action simulates when an update rollback fails as a user must manually delete problematic resources before continuing an update rollback.

$$ManuallyDeleteResources \triangleq \land status = UPDATE\_ROLLBACK\_FAILED \land status' = UPDATE\_ROLLBACK\_IN\_PROGRESS$$

Ongoing removal of new resources for one or more stacks after a failed stack update. In this state, the stack has been rolled back to its previous working state and is usable, but *AWS CloudFormation* is still deleting any new resources it created during the stack update.

$$UpdateRollbackCompleteCleanupInProgress \triangleq \land status = UPDATE\_ROLLBACK\_IN\_PROGRESS \land status' = UPDATE\_ROLLBACK\_COMPLETE\_CLEANU$$

Next state relation.

$$\begin{aligned} Next \triangleq\ & \lor CreateInProgress \\ & \lor CreateComplete \\ & \lor CreateFailed \\ & \lor DeleteInProgress \\ & \lor DeleteComplete \\ & \lor DeleteFailed \\ & \lor UpdateInProgress \\ & \lor UpdateComplete \\ & \lor UpdateCompleteCleanupInProgress \\ & \lor RollbackInProgress \\ & \lor RollbackComplete \\ & \lor RollbackFailed \\ & \lor UpdateRollbackInProgress \\ & \lor UpdateRollbackComplete \\ & \lor UpdateRollbackFailed \\ & \lor ManuallyDeleteResources \\ & \lor UpdateRollbackCompleteCleanupInProgress \end{aligned}$$

$$Spec \triangleq Init \land \Box[Next]_{vars}$$

THEOREM $Spec \Rightarrow \Box TypeInvariant$

* Modification History
* Last modified Sun May 19 18:18:58 *PDT* 2019 by *jasondebolt*
* Created Sun May 19 15:44:54 *PDT* 2019 by *jasondebolt*