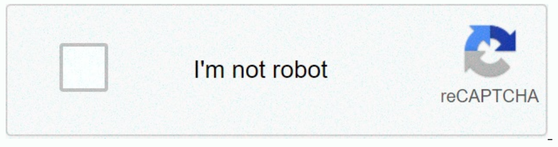

Continue

Cloudformation template assume role

I am trying to solve the logical flow of an AWS CloudFormation template that will assume an IAM role that can remove files from an S3 cube in another AWS account. What I have so far is: accountA has a roleA roleA has a policy that allows sts:AssumeRole for a role in accountB :arn:aws:iam::1112223344:role/AllowPullS3 accountB has paper (AllowPullS3) with the policy allow:s3 listBucket + get,put,delete trust relationship for accountA :Action:sts:AssumeRole If I create an EC2 instance manually with IAM:roleA and then use the CLI to get the assume function credentials, I can remove the files from the S3 cube from the other account as expected. But what should I put where in my account A cf template that will allow the EC2 instance to take on roleB and remove the file from the S3 accountB bucket as part of the training? I've tried following a lot of tutorials like this cfn-iam:init tutorial but still can't fully grasp what's going on. Thanks for your advice. Art Creates a new role for your AWS account. For more information about features, go to IAM Functions. For information about the limitations of role names and the number of roles you can create, go to IAM Entity Limitations in the IAM User Guide. Syntax To declare this entity to your AWS CloudFormation template, use the following syntax: { Type : AWS::IAM::Role, Properties : { AssumeRolePolicyDocument: Json, Description : String, ManagedPolicyArns: [String, ...], MaxSessionDuration: Integer, Path : String, PermissionsBoundary : String, Policies : [Politics, ...], RoleName : String, Tags : [Tag, AssumeRolePolicyDocument Properties The trust policy associated with this role. Trust policies define which entities can take on the role. You can only associate a trusted policy with a role. For an example of a rule that can be used to assume a role, see Template examples. For more information about the items you can use in an IAM policy, see reference IAM policy elements in the IAM User Guide. Required: Yes Type: Json Update requires: No interruption Description A description of the role you provide. Required: No Type: Maximum String: 1000 Pattern: [\p {L}\p{M}\p{Z}\p{S}\p{N}\p{P}]* The update requires: No Interrupt ManagedPolicyArns A list of Amazon Resource Names (ARDRs) of the IAM-managed policies you want to attach to the user. For more information about RNA, see Amazon Resource Names (RNA) and AWS service namespaces in the AWS general reference. Required: No Type: The string update list requires: No MaxSessionDuration interrupt The maximum session duration (in seconds) you want to set for the specified function. If you do not specify a value for this the default maximum of one hour will be applied. This option can have a value of 1 hour to 12 hours. Anyone who assumes the role from the AWS CLI or API can use the DurationSeconds API parameter or the second duration CLI parameter to request a longer session. The determines the maximum duration that can be requested using the DurationSeconds parameter. If users do not specify a value for the DurationSeconds parameter, their security credentials are valid for a default time. This applies when you use assumerole* API operations or role-taking operations* CLI, but does not apply when you use these operations to create a console URL. For more information, see Using IAM features in the IAM User Guide. Required: No type: Enter Minimum: 3600 Maximum: 43200 The update requires: No interrupt path The path to the function. For more information about paths, see IAM identifiers in the IAM User Guide. This parameter is optional. If not included, it is not in a slash (/) by default. This parameter allows (through its regex pattern) a string of characters consisting of a slash (/) by itself or a string that must start and end with forward slashes. In addition, it can contain any ASCII character from the ! (\u0021) through the DEL character (\u007F), including most punctuation characters, upper and lower digits and letters. Required: No type: Minimum string: 1 Maximum: 512 Pattern: (\u002F)| (\u002F[\u0021-\u007F]+\u002F) The update requires: Replacement permissionsBoundary The RNA of the policy used to set the permission limit for the role. For more information about permission limits, see Permission limits for IAM identities in the IAM User Guide. Required: No type: String update requires: No interrupt policies Add or update an online policy document that is embedded in the specified IAM function. When you insert an online policy on paper, the online policy is used as part of the function's access rule (permissions). Paper trust policy is created at the same time as paper. You can update the trust policy for a role later. For more information about IAM functions, go to Using Roles to Delegate Federated Permissions and Identities. A role can also have a managed policy attached. For policy information, see Managed Policies and Online Policies in the IAM User Guide. For information about the limits on the number of online policies you can insert with a role, see Limitations on IAM entities in the IAM User Guide. If an external policy (such as AWS::IAM::P olicy or AWS::IAM::ManagedPolicy) has a Ref in a role and if a resource (such as AWS::ECS::Service) also has a Ref in the same role, add a DependsOn attribute to the resource to make the resource dependent on external policy. This dependency ensures that the paper policy is available throughout the resource's life cycle. For example, when a stack with an AWS resource::ECS::Service, the DependsOn attribute ensures that AWS CloudFormation removes the AWS::ECS::Service resource before deleting the policy from its role. Required: No type: The policy update list requires: There is no interrupt RoleName name for the IAM function. For valid values, see the RoleName parameter for the CreateRole action in the IAM User Guide. This parameter (for its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters without spaces. You can also include any of the following characters: _+=,.@-. The role name must be unique in the account. Role names are not case sensitive. For example, you cannot create role1 and role1 roles. If you do not specify a name, AWS CloudFormation generates a unique physical identifier and uses this identifier for the function name. If you specify a name, you must specify CAPABILITY_NAMED_IAM value to recognize the capabilities of the template. For more information, see Recognizing IAM resources in AWS cloudformation templates. The name of an IAM resource can cause an unrecoverable error if you use the same template again in multiple regions. To avoid this, we recommend using Fn::Join and AWS::Region to create a region-specific name, as in the following example: {Fn::Join: [, [{Ref: AWS::Region}, {Ref: MyResourceName}]]}. Required: No Type: String Update Requires: Replacement Labels A list of labels that are attached to the specified function. For more information about tagging, see Tagging IAM identities in the IAM User Guide. Required: No Type: Maximum Tag List: 50 Update Requires: No Interrupt Ref Return Values When providing this resource's logical ID to the intrinsic Ref function, Ref returns the resource name. For example: { Ref: RootRole } For AWS::IAM::Role resource with the logical RootRole ID, Ref will return the function name. For more information about using the Ref function, see Ref. Fn::GetAtt The Fn::GetAtt function returns a value for a specified attribute of this type. The following are the available attributes and sample return values. For more information about using the intrinsic function Fn::GetAtt, see Fn::GetAtt. Arn returns the name of the Amazon resource (RNA) for the feature. For example: {Fn::GetAtt : [MyRole, Arn] } This will return a value such as rna:aws:iam::1234567890:role/MyRole-AJJHDSKSDF. RoleId Returns the stable and unique string identifying the function. For example, AIDAJQABLZS4A3QDU576Q. For more information about IDs, see IAM identifiers in the IAM User Guide. Examples of IAM function with policy profiles and embedded instances This example shows a policy embedded in the AWS::IAM::Role. The policy is specified online in the AWS Policies property::IAM::Role. { AWSTemplateFormatVersion: 2010-09-09, Resources: { RootRole: { Type: AWS::IAM::Role, Properties: { AssumeRolePolicyDocument. : { Version: 2012-10-17, Statement: [{ Effect: Allow, Main: { Service: [ec2.amazonaws.com] }, Action: [sts:AssumeRole] } } } } } } } } Path: /, Policies: [[PolicyName: root, PolicyDocument: { Version: 2012-10-17, Statement: [[Allow, Action: *, Resource: * } } } } } } }, RootInstanceProfile: { Type: AWS::IAM::InstanceProfile, Properties: { Path: /, Roles: [{ Ref: RootRole } } } } } } } 2010-09-09 Resources: RootRole: Type: 'AWS::IAM::Role' Properties: AssumeRolePolicyDocument: Version: 2012-10-17 Statement: - Effect: Allow Main: Service: - ec2.amazonaws.com Action: - 'sts:AssumeRole ' Path: / Policies: - PolicyName: root PolicyDocument: Version: 2012-10-17 Statement: - Effect: Allow action: '*' Resource: '*' RootInstanceProfile: Type: 'AWS::IAM::InstanceProfile' Properties: Path: / Roles: - ! Ref RootRole IAM Function with External Policy Profiles and Instance In this example, the policy and instance resources are specified externally in the IAM function. They refer to the function by specifying their name, RootRole, in their respective function properties. { AWSTemplateFormatVersion: 2010-09-09, Resources: { RootRole: { Type: AWS::IAM::Role, Properties: { AssumeRolePolicyDocument. : { Version : 2012-10-17, Statement: [[Effect: Allow, Main: { Service: [ec2.amazonaws.com] }, Action: [sts:AssumeRole] } } } } } } } } } } } } Path: / } }, RolePolicies: { Type: AWS::IAM::P olicy, Properties: { PolicyName: root, PolicyDocument: { Version: 2012-10-17, Statement: [[Effect: Allow, Action: *, Resource: * } } }, Roles: [Ref: RootRole } } } }, RootInstanceProfile: { Type: AWS::IAM::InstanceProfile, Properties: { Path: /, Roles: [[Ref: RootRole } } } } } } } } AWSTemplateFormatVersion: 2010-09-09 Resources: RootRole: Type: AWS::IAM::Role Properties: AssumeRolePolicyDocument: Version: 1 Statement from 2012-10-17: - Effect: Allow Main: Service: - Action ec2.amazonaws.com: - sts:AssumeRole Way: / RolePolicies: Type: AWS:::IAM::P olicy Properties: PolicyName: root PolicyDocument: Version: 2012-10-17 Statement: - Effect: Allow Action: * Resources: * Roles: - Ref: RootRole RootInstanceProfile: Type: AWS::IAM::InstanceProfile Properties: Path: / Roles: - Ref: RootRole See also helped you this page? - Yes Thank you for leting us know that we are doing a good job! If you have a moment, please tell us what we did well so we can do more of it. Did this page help you? - No thanks for leting us know that this page needs work. We're sorry we let you down. If you have a moment, tell us how we can improve the documentation. Best.