SCA configureren voor samenvoeging van meerdere AWS-accounts via één AWS S3-emmer

Inhoud

Inleiding

Dit document beschrijft hoe u een Amazon Web Services (AWS) Simple Storage Service (S3) configureert om logbestanden van een tweede AWS-account te accepteren.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Secure Cloud-analyses
- AWS Identity Access Management (IAM)
- AWS S3-software

Gebruikte componenten

De informatie in dit document is gebaseerd op:

- AWS Account A (aangeduid als ACCOUNT_A_ID - Deze account host/is eigenaar van de

reeds bestaande S3-emmers)
- AWS Account B (aangeduid als ACCOUNT_B_ID - Dit is een nieuw account (naar Secure Cloud Analytics) dat gegevens verstuurt naar ACCOUNT_A_ID's S3_BUCKET_NAME)
- Secure Cloud-analyse (moet al worden geïntegreerd met ACCOUNT_A_ID)

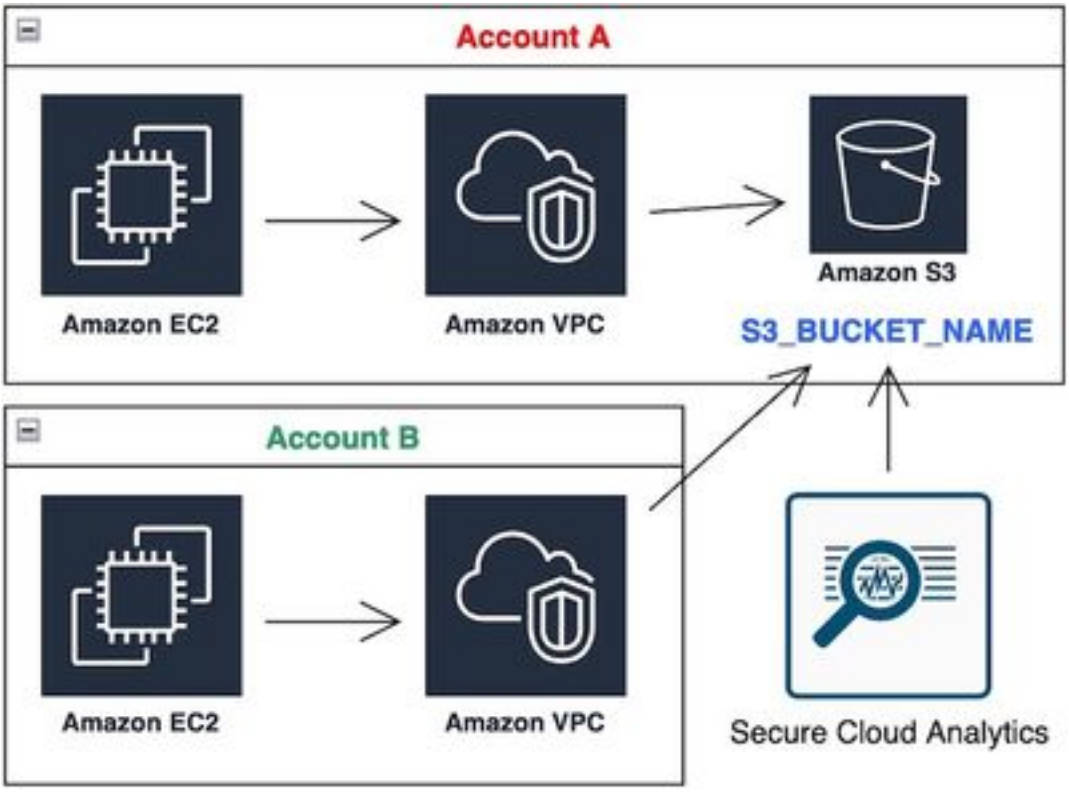
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configureren

Er zijn vijf stappen om SCA inneemt 2+ accounts van 1 S3 emmer:

1. Bijwerken **ACCOUNT_A_ID's S3_BUCKET_NAME** subsidiebeleid **ACCOUNT_B_ID** schrijfrechten voor account.
2. Configureer de **ACCOUNT_B_ID** account voor verzenden van VPC Flow Logs naar **ACCOUNT_A_ID's S3_BUCKET_NAME**.
3. IAM-beleid maken in **ACCOUNT_B_ID's** AWS IAM-dashboard.
4. IAM-rol maken in **ACCOUNT_B_ID's** AWS IAM-dashboard.
5. Secure Cloud-analysereferenties configureren voor **ACCOUNT_B_ID**.

Netwerkdiagram



Gegevensstroomdiagram

Configuraties

1. Update ACCOUNT_A_ID's S3_BUCKET_NAME Beleid om ACCOUNT_B_ID Account schrijfrechten te verlenen

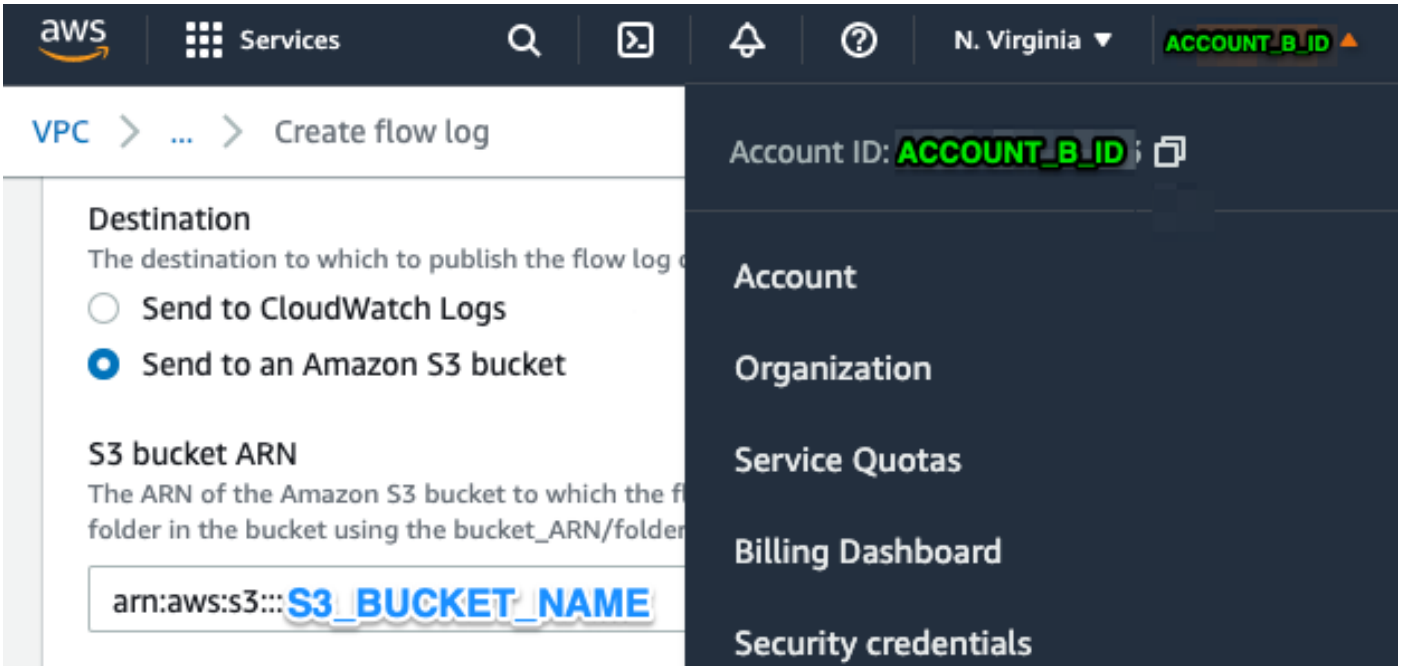
ACCOUNT_A_ID's S3_BUCKET_NAME de configuratie van het emmerbeleid wordt hier verstrekt. Deze configuratie maakt het mogelijk om een secundaire (of een willekeurig aantal accounts dat u wenst) account te schrijven (SID-AWSLogDeliveryWrite) naar de S3 emmer, en om ACL's (SID - AWSLogDeliveryAclCheck) te controleren voor de emmer.

- Wijzigen **ACCOUNT_A_ID** en **ACCOUNT_B_ID** hun respectieve numerieke waarden zonder streepjes.
- Wijzigen **S3_BUCKET_NAME** de respectieve naam van de emmer.
- Negeer hier de opmaak, AWS kan deze naar wens bewerken.

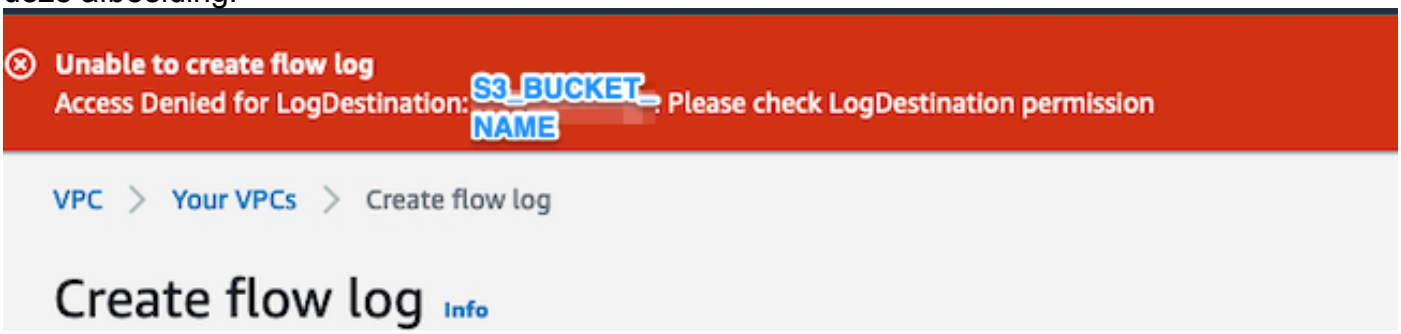
```
{
"Version": "2012-10-17",
"Statement": [
{
"Sid": "AWSLogDeliveryWrite",
"Effect": "Allow",
"Principal": {"Service": "delivery.logs.amazonaws.com"},
"Action": "s3:PutObject",
"Resource": ["arn:aws:s3:::S3_BUCKET_NAME","arn:aws:s3:::S3_BUCKET_NAME/*"],
"Condition": {
"StringEquals": {"aws:SourceAccount": ["ACCOUNT_A_ID","ACCOUNT_B_ID"]},
"ArnLike": {"aws:SourceArn": ["arn:aws:logs:*:ACCOUNT_A_ID:*","arn:aws:logs:*:ACCOUNT_B_ID:*"]}
}
},
{
"Sid": "AWSLogDeliveryAclCheck",
"Effect": "Allow",
"Principal": {
"Service": "delivery.logs.amazonaws.com"
},
"Action": "s3:GetBucketAcl",
"Resource": "arn:aws:s3:::S3_BUCKET_NAME",
"Condition": {
"StringEquals": {"aws:SourceAccount": ["ACCOUNT_A_ID","ACCOUNT_B_ID"]},
"ArnLike": {"aws:SourceArn": ["arn:aws:logs:*:ACCOUNT_A_ID:*","arn:aws:logs:*:ACCOUNT_B_ID:*"]}
}
}
]
}
```

2. Het Account_B_ID configureren om VPC Flow Logs naar de S3_BUCKET_NAME van ACCOUNT_A_ID te sturen

Een VPC Flow Log maken **ACCOUNT_B_ID** die **ACCOUNT_A_ID'sS3_BUCKET_NAME** emmer ARN in de bestemming zoals in deze afbeelding:



Als de permissies op de S3 emmer niet goed zijn ingesteld, dan ziet u een fout vergelijkbaar met deze afbeelding:



3. Maak een IAM-beleid aan in het AWS IAM Dashboard van ACCOUNT_B_ID

De IAM Policy-configuratie die is gekoppeld aan de swc_role op **ACCOUNT_B_ID** is:

```
swc_single_policy
{
"Version": "2012-10-17",
"Statement": [
{
"Action": [
"autoscaling:Describe*",
"cloudtrail:LookupEvents",
"cloudwatch:Get*",
"cloudwatch:List*",
"ec2:Describe*",
"ecs:List*",
"ecs:Describe*",
"elasticache:Describe*",
"elasticache:List*",
"elasticloadbalancing:Describe*",
"guardduty:Get*",
"guardduty:List*",
"iam:Get*",
"iam:List*",
"inspector:*",
```

```
"rds:Describe*",
"rds:List*",
"redshift:Describe*",
"workspaces:Describe*",
"route53:List*"
],
"Effect": "Allow",
"Resource": "*"
},
{
"Action": [
"logs:Describe*",
"logs:GetLogEvents",
"logs:FilterLogEvents",
"logs:PutSubscriptionFilter",
"logs:DeleteSubscriptionFilter"
],
"Effect": "Allow",
"Resource": "*"
},
{
"Sid": "CloudCompliance",
"Action": [
"access-analyzer:ListAnalyzers",
"cloudtrail:DescribeTrails",
"cloudtrail:GetEventSelectors",
"cloudtrail:GetTrailStatus",
"cloudtrail:ListTags",
"cloudwatch:DescribeAlarmsForMetric",
"config:Get*",
"config:Describe*",
"ec2:GetEbsEncryptionByDefault",
"iam:GenerateCredentialReport",
"iam:Get*",
"iam:List*",
"kms:GetKeyRotationStatus",
"kms:ListKeys",
"logs:DescribeMetricFilters",
"logs:Describe*",
"logs:GetLogEvents",
"logs:FilterLogEvents",
"organizations:ListPolicies",
"s3:GetAccelerateConfiguration",
"s3:GetAccessPoint",
"s3:GetAccessPointPolicy",
"s3:GetAccessPointPolicyStatus",
"s3:GetAccountPublicAccessBlock",
"s3:GetAnalyticsConfiguration",
"s3:GetBucket*",
"s3:GetEncryptionConfiguration",
"s3:GetInventoryConfiguration",
"s3:GetLifecycleConfiguration",
"s3:GetMetricsConfiguration",
"s3:GetObjectAcl",
"s3:GetObjectVersionAcl",
"s3:GetReplicationConfiguration",
"s3:ListAccessPoints",
"s3:ListAllMyBuckets",
"securityhub:Get*",
"sns:ListSubscriptionsByTopic"
],
"Effect": "Allow",
"Resource": "*"
},
```

```
{
"Action": [
"s3:ListBucket",
"s3:GetBucketLocation",
"s3:GetObject"
],
"Effect": "Allow",
"Resource": [
"arn:aws:s3:::S3_BUCKET_NAME/*",
"arn:aws:s3:::S3_BUCKET_NAME"
]
}
]
}
```

4. Maak een IAM Role aan in het AWS IAM Dashboard van ACCOUNT_B_ID

1. Selecteer **Roles**.

2. Selecteer **Create role**.

3. Selecteer het roltype andere AWS-account.

4. Voer in het veld Account-ID 757972810156 in.

5. Selecteer de optie Externe ID vereisen.

6. Voer de naam van uw Secure Cloud Analytics-webportal in als de **External ID**.
7. Klik op **Next: Permissions .**

8. Selecteer de **swc_single_policy** beleid dat u zojuist hebt gemaakt.

9. Klik op **Next: Tagging**.

10. Klik op **Next: Review**.

11. Voer swc_role in als de naam van de rol.

12. Voer een **Description**, zoals Rol om toegang tot kruisrekeningen mogelijk te maken.

13. Klik op **Create role** .

14. Kopieer de rol ARN en plak het in een platte editor.

5. Secure Cloud Analytics-referenties voor ACCOUNT_B_ID configureren

1. Log in op Secure Cloud Analytics en selecteer **Settings > Integrations > AWS > Credentials**.

2. Klik op **Add New Credentials**.

3. Voor de **Name**, voorgestelde naamgevingsschema zou **Account_B_ID_creds** (bijvoorbeeld; 012345678901_creds) voor elke account, wilt u innemen.

4. Plakt de rol ARN uit de vorige stap en plak deze in het **Role ARN** veld.

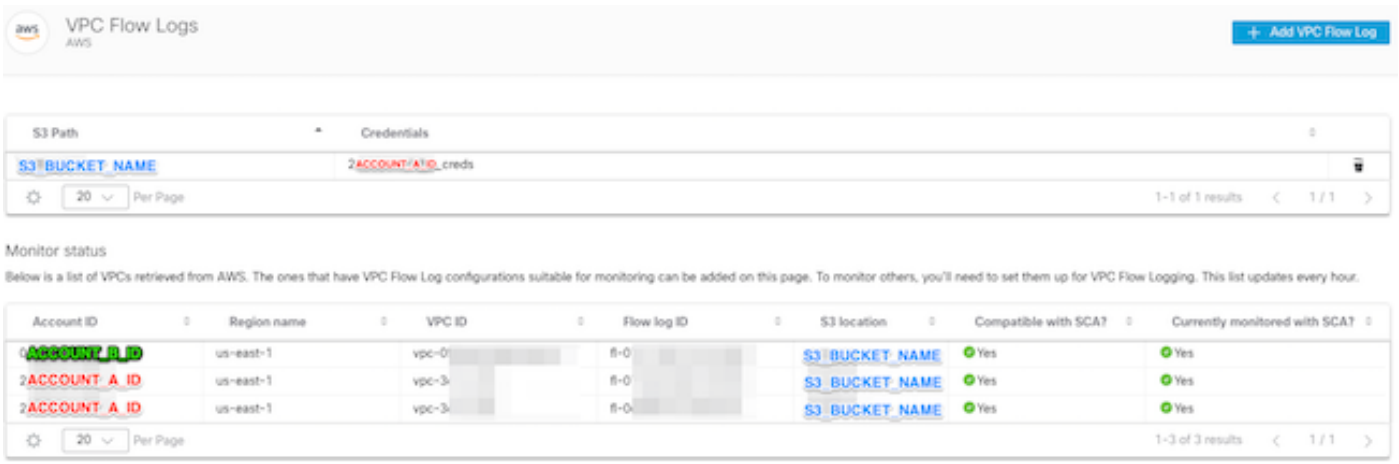
5. Klik **Create**.

Er zijn geen verdere configuratiestappen vereist.

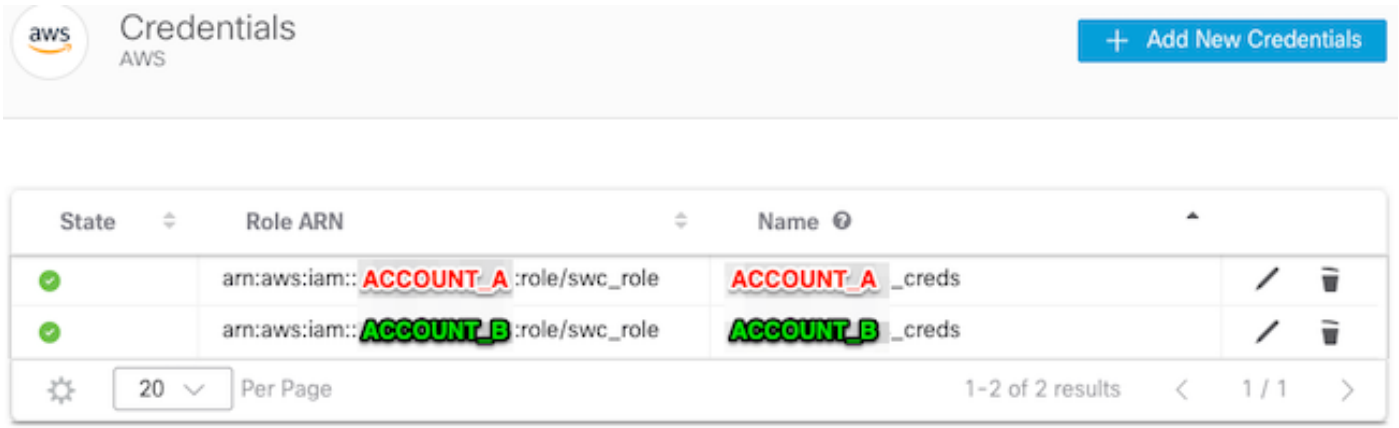
Verifiëren

Gebruik deze sectie om te controleren of uw configuratie goed werkt.

Uw VPC Flow Logs pagina in uw Secure Cloud Analytics webpagina ziet er na ongeveer een uur zo uit als deze afbeelding. URL naar VPC Flow Logs pagina: **https://portal-name.obsrvbl.com/v2/#/settings/integrations/aws/vpc_logs**



Uw AWS Credentials pagina ziet er als volgt uit:



Problemen oplossen

Deze sectie bevat informatie die u kunt gebruiken om problemen met de configuratie te troubleshooten.

Als u niet dezelfde resultaten ziet op uw VPC Flow Log pagina, moet u AWS S3 Server Access Vastlegging inschakelen.

Voorbeelden van S3 Server Access Logging (SCA sensor GET-ing gegevens van S3):

acfb735656a2b1bbd16c05582b753d11a9306f3a8dc20a4b9edc8c999aef9dd2 S3_BUCKET_NAME [10/Apr/2022:22:55:12 +0000] 10.0.129.197 arn:aws:sts::ACCOUNT_A_ID:assumed-role/swc_role/b401ed3c-58d1-472d-ab20-4801d0a7 CSQPM6SB0YZNWE03 REST.GET.BUCKET - "GET /?list-type=2&delimiter=%2F&prefix=AWSLogs%2FACCOUNT_B_ID%2Fvpcflowlogs%2F&encoding-type=url HTTP/1.1" 200 - 421 - 13 13 "-" "Boto3/1.17.85 Python/3.6.9 Linux/5.4.0-1064-aws Botocore/1.20.85" - ghD4o28lk0G1X3A33qCtXIg4qDRfo4eN3uebyV+tdCBQ6tOHk5XvLHGwbd7/EKXdzX+6PQxLHys= SigV4 ECDHE-RSA-AES128-GCM-SHA256 AuthHeader S3_BUCKET_NAME.s3.amazonaws.com TLSv1.2 -
acfb735656a2b1bbd16c05582b753d11a9306f3a8dc20a4b9edc8c999aef9dd2 S3_BUCKET_NAME [10/Apr/2022:22:55:12 +0000] 10.0.129.197 arn:aws:sts::ACCOUNT_A_ID:assumed-role/swc_role/b401ed3c-58d1-472d-ab20-4801d0a7 CSQTXPDG4G6MY2CR REST.GET.BUCKET - "GET /?list-type=2&delimiter=%2F&prefix=AWSLogs%2F&encoding-type=url HTTP/1.1" 200 - 445 - 33 33 "-" "Boto3/1.17.85 Python/3.6.9 Linux/5.4.0-1064-aws Botocore/1.20.85" - geCd2CjQUqwxYjVs0JUt+gyEuKw92p3iJt52qx0A+bOaWhjaiNI77OxGqmvFlJZpMT5GePh6i9Y= SigV4 ECDHE-RSA-AES128-GCM-SHA256 AuthHeader S3_BUCKET_NAME.s3.amazonaws.com TLSv1.2 -
acfb735656a2b1bbd16c05582b753d11a9306f3a8dc20a4b9edc8c999aef9dd2 S3_BUCKET_NAME [10/Apr/2022:22:55:12 +0000] 10.0.129.197 arn:aws:sts::ACCOUNT_A_ID:assumed-role/swc_role/b401ed3c-58d1-472d-ab20-4801d0a7 CSQVVKEPV0XD9987 REST.GET.BUCKET - "GET /?list-type=2&delimiter=%2F&prefix=AWSLogs%2FACCOUNT_A_ID%2Fvpcflowlogs%2F&encoding-type=url HTTP/1.1" 200 - 421 - 11 11 "-" "Boto3/1.17.85 Python/3.6.9 Linux/5.4.0-1064-aws Botocore/1.20.85" - hHR2+J5engOwp/Bi7Twn5ShsDXNYnH5rcB8YByFJP5OnZb64S1Y7/d+c7BSbBb861TpuJ0Jtpes= SigV4 ECDHE-RSA-AES128-GCM-SHA256 AuthHeader S3_BUCKET_NAME.s3.amazonaws.com TLSv1.2 -

Referentie logveld: https://docs.aws.amazon.com/AmazonS3/latest/userguide/LogFormat.html

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.