Configurazione di SCA per l'acquisizione di più account AWS tramite un singolo bucket AWS S3

Sommario

Introduzione

In questo documento viene descritto come configurare un servizio di archiviazione semplice (S3) Amazon Web Services (AWS) in modo che accetti i log da un secondo account AWS.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Secure Cloud Analytics
- AWS Identity Access Management (IAM)
- AWS-S3

Componenti usati

Le informazioni fornite in questo documento si basano su:

- Account AWS A (indicato come ACCOUNT_A_ID - Questo account possiede i bucket S3 già esistenti)
- Account AWS B (indicato come ACCOUNT_B_ID - Si tratta di un nuovo account (per Secure

Cloud Analytics) che invia dati a S3_BUCKET_NAME di ACCOUNT_A_ID)
- Secure Cloud Analytics (deve già essere integrato con ACCOUNT_A_ID)

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Esistono cinque fasi per avere conti SCA ingest 2+ da 1 bucket S3:

1. Update **ACCOUNT_A_ID's S3_BUCKET_NAME** politica da concedere **ACCOUNT_B_ID** autorizzazioni di scrittura dell'account.
2. Configurare **ACCOUNT_B_ID** account a cui inviare i log di flusso VPC **ACCOUNT_A_ID's S3_BUCKET_NAME**.
3. Crea criterio IAM in **ACCOUNT_B_ID's** Dashboard AWS IAM.
4. Crea ruolo IAM in **ACCOUNT_B_ID's** Dashboard AWS IAM.
5. Configurare le credenziali di Secure Cloud Analytics per **ACCOUNT_B_ID**.

Esempio di rete

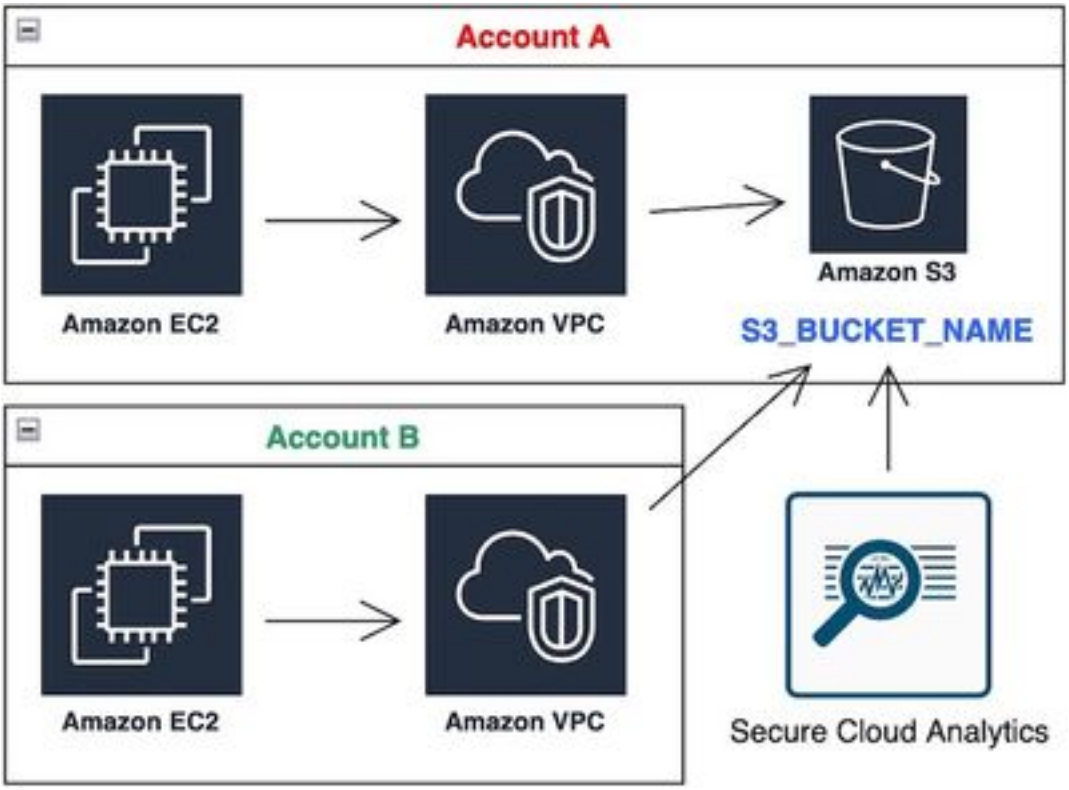


Diagramma di flusso dei dati

Configurazioni

1. Aggiornare il criterio S3_BUCKET_NAME di ACCOUNT_A_ID per concedere le autorizzazioni di scrittura dell'account ACCOUNT_B_ID

ACCOUNT_A_ID's S3_BUCKET_NAME configurazione dei criteri bucket fornita qui. Questa configurazione consente a un account secondario (o a un numero qualsiasi di account desiderato) di scrivere

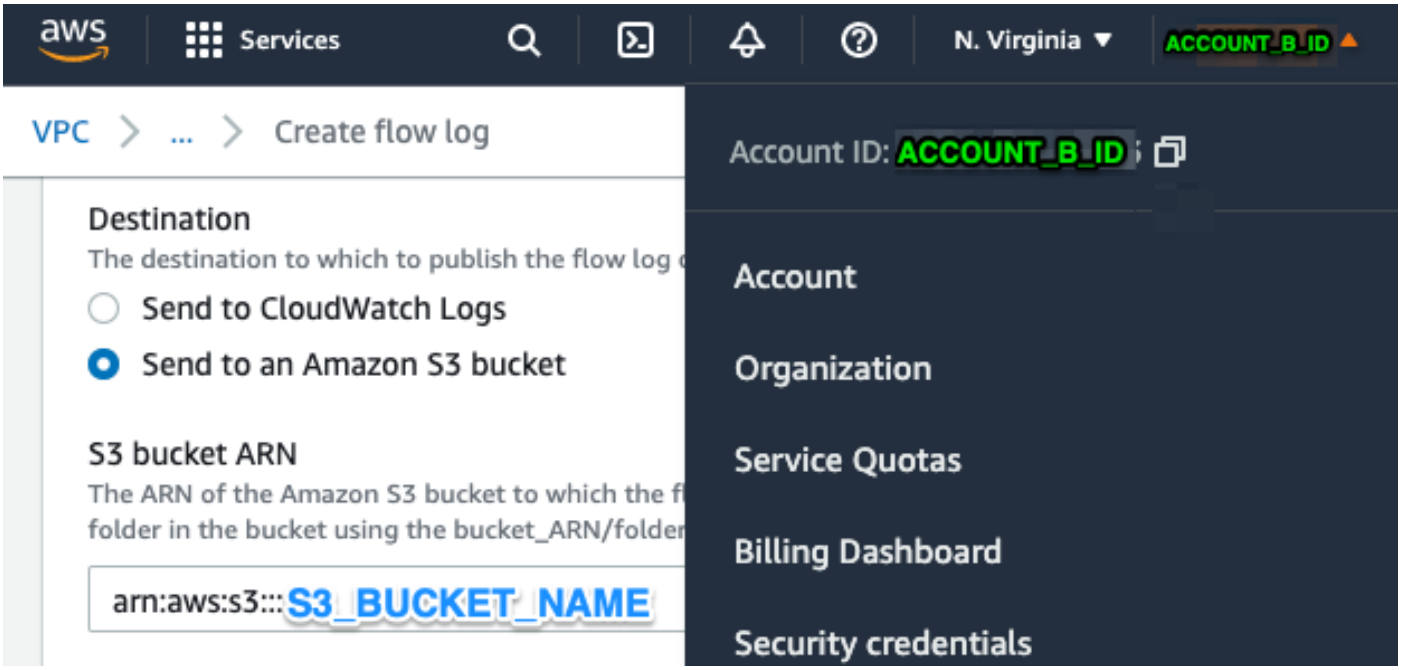
(SID-AWSLogDeliveryWrite) nel bucket S3 e di controllare gli ACL (SID - AWSLogDeliveryAclCheck) per il bucket.

- Cambia **ACCOUNT_A_ID** e **ACCOUNT_B_ID** ai rispettivi valori numerici senza trattini.
- Cambia **S3_BUCKET_NAME** al nome del rispettivo bucket.
- Ignorare la formattazione. AWS può modificarla in base alle esigenze.

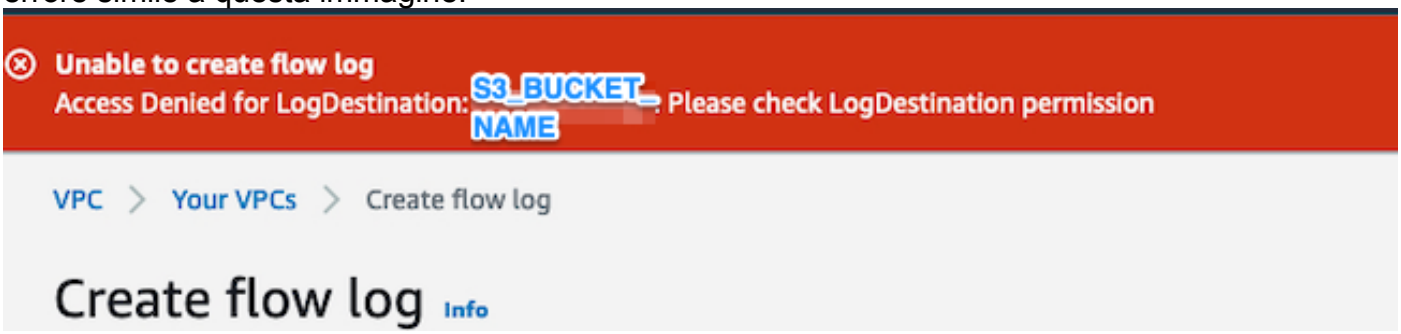
```
{
"Version": "2012-10-17",
"Statement": [
{
"Sid": "AWSLogDeliveryWrite",
"Effect": "Allow",
"Principal": {"Service": "delivery.logs.amazonaws.com"},
"Action": "s3:PutObject",
"Resource": ["arn:aws:s3:::S3_BUCKET_NAME","arn:aws:s3:::S3_BUCKET_NAME/*"],
"Condition": {
"StringEquals": {"aws:SourceAccount": ["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. Configurare l'account ACCOUNT ACCOUNT_B_ID per inviare i log di flusso VPC all'account S3_BUCKET_NAME di ACCOUNT_A_ID

Creazione di un registro di flusso VPC **ACCOUNT_B_ID** che ha **ACCOUNT_A_ID'sS3_BUCKET_NAME** bucket ARN nella destinazione come mostrato in questa immagine:



Se le autorizzazioni sul bucket S3 non sono configurate correttamente, viene visualizzato un errore simile a questa immagine:



3. Creare i criteri IAM nel dashboard AWS IAM di ACCOUNT_B_ID

Configurazione dei criteri IAM associata a swc_role in **ACCOUNT_B_ID** è:

```
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. Creare il ruolo IAM nel dashboard AWS IAM di ACCOUNT_B_ID

1. Selezionare **Roles**.

2. Selezionare **Create role**.

3. Selezionare il tipo di ruolo Altro account AWS.

4. Inserire 757972810156 nel campo ID account.

5. Selezionare l'opzione Richiedi ID esterno.

6. Immettere il nome del portale Web di Secure Cloud Analytics come **External ID**.
7. Fare clic su **Next: Permissions .**

8. Selezionare il **swc_single_policy** criterio appena creato.

9. Fare clic su **Next: Tagging**.

10. Fare clic su **Next: Review**.

11. Inserire swc_role come nome del ruolo.

12. Inserire un **Description**, ad esempio un ruolo per consentire l'accesso tra account.

13. Fare clic su **Create role** .

14. Copiare il ruolo ARN e incollarlo in un editor di testo normale.

5. Configurare le credenziali di Secure Cloud Analytics per ACCOUNT_B_ID

1. Accedi a Secure Cloud Analytics e seleziona **Settings > Integrations > AWS > Credentials**.

2. Fare clic su **Add New Credentials**.

3. Per il **Name**, lo schema di denominazione consigliato **Account_B_ID_creds** (ad esempio; 012345678901_creds) per ciascun account che si desidera acquisire.

4. Incollare il ruolo ARN dal passo precedente e incollarlo nel **Role ARN** campo.

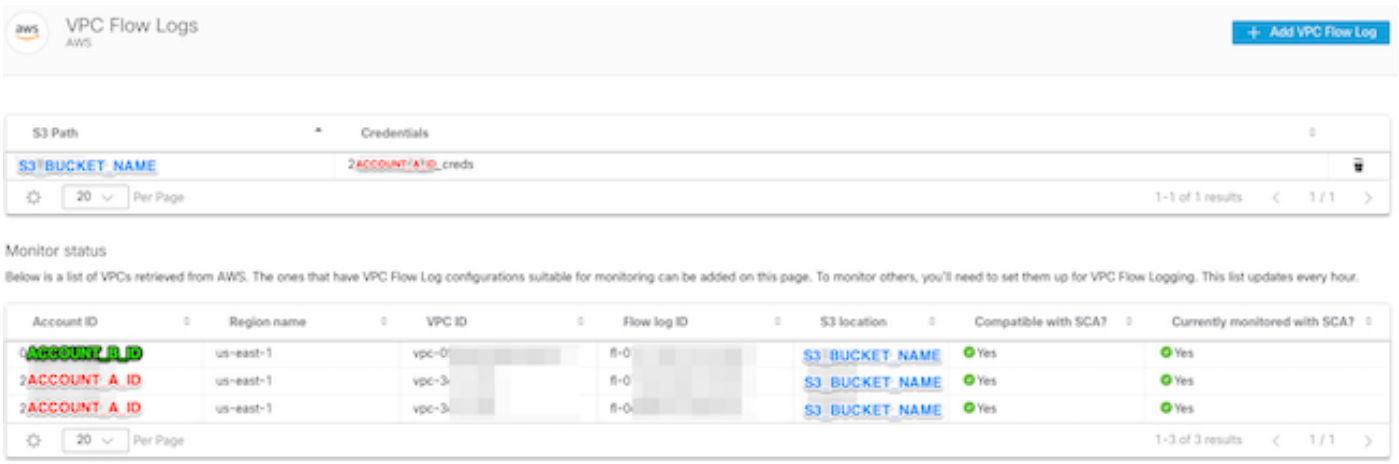
5. Clic **Create**.

Non sono necessari ulteriori passaggi di configurazione.

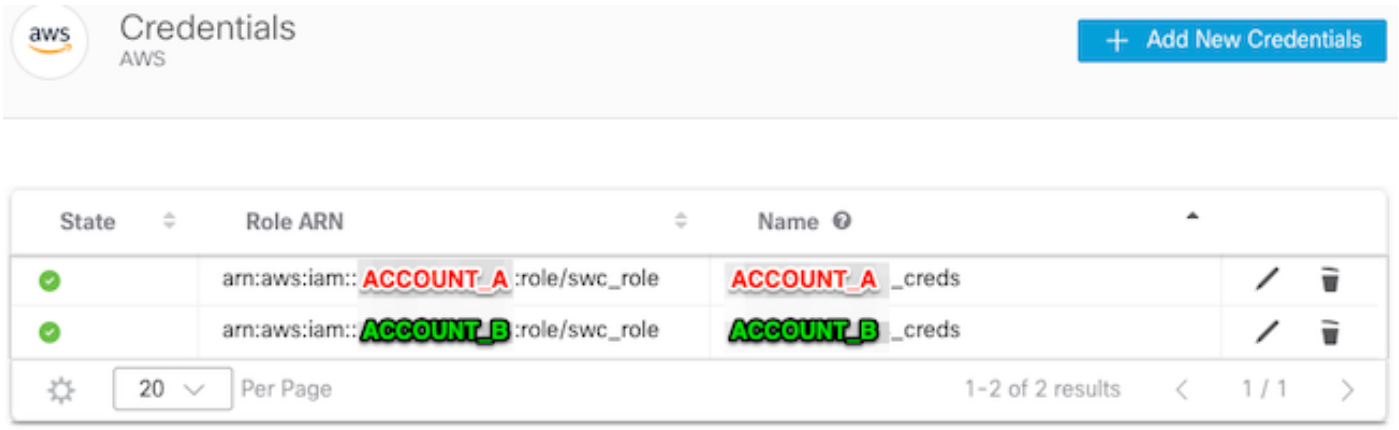
Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

La pagina VPC Flow Logs nella pagina Web Secure Cloud Analytics ha l'aspetto di questa immagine dopo circa un'ora. URL della pagina VPC Flow Logs: **https://portal-name.obsrvbl.com/v2/#/settings/integrations/aws/vpc_logs**



La pagina Credenziali AWS ha il seguente aspetto:



Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Se nella pagina VPC Flow Log non vengono visualizzati gli stessi risultati, è necessario abilitare la registrazione degli accessi al server di AWS S3.

Esempi di registrazione accesso server S3 (sensore SCA GET-ing dati da 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 -

Riferimento campo registro:
https://docs.aws.amazon.com/AmazonS3/latest/userguide/LogFormat.html

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).