Create a Remote Log Source - AWS WAF

Armor Knowledge Base

Topics Discussed

To obtain Log Relay and to configure your account for remote log collection, you must have the following AMP permissions added to your account:

- Write Virtual Machine
- Delete Log Management
- Read Log Endpoints
- Read Log Relays
- Write Log Relays
- Delete Log Relays

You can use this document to collect and send AWS WAF logs to Armor's Security Information & Event Management (SIEM).

Pre-Deployment Considerations

Before you begin, review the following requirements:

AMP Permissions

Your Armor Management Portal (AMP) account must have the following permissions:

- Write Virtual Machine
- Delete Log Management
- Read Log Endpoints
- Read Log Relays
- Write Log Relays
- Delete Log Relays

To learn more about permissions in AMP, see Roles and Permissions.

Log Relay

For remote log collection, you must have a Log Relay server on your account.

- To learn how to add Log Relay to your account, see Obtain Log Relay for Remote Log Collection.

AWS Account Permissions (Policies)

Your AWS service account must have full access to AWS CloudWatch.

Your individual AWS user account must have full access to the following AWS features:

- AWS WAF
- AWS Lambda
- AWS CloudWatch
- AWS CloudFormation

Web ACL

To ingest logs from an AWS WAF, you must first configure a **Web ACL**.

- To learn how to create a **Web ACL**, see AWS's documentation site.

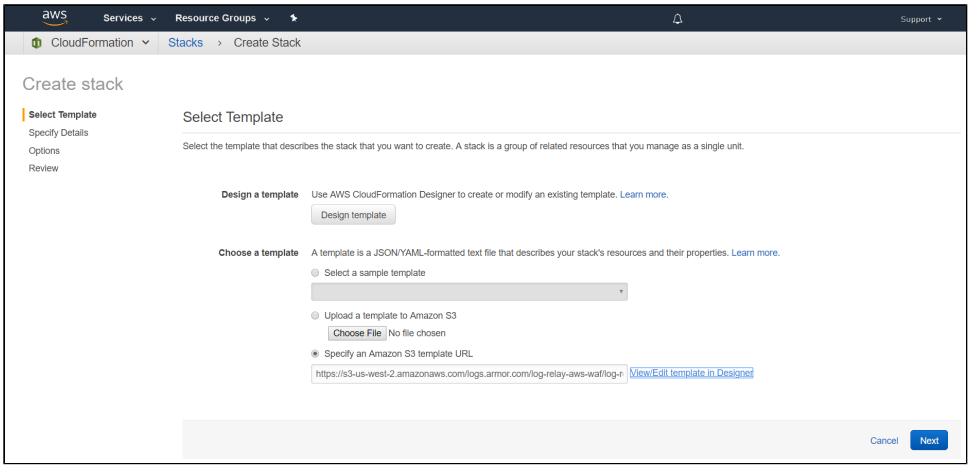
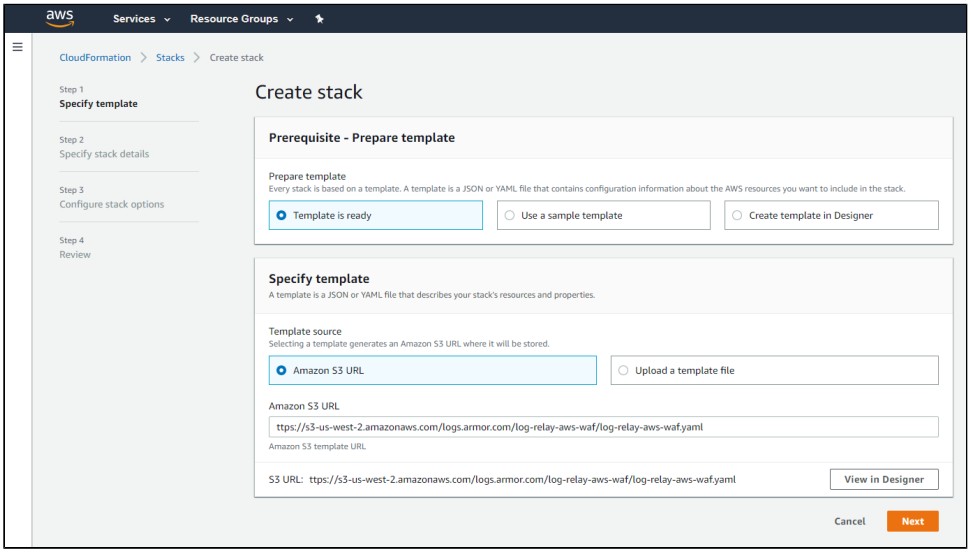
> Armor does not provide support for using AWS CloudFormation to set up AWS WAF resources in AWS GovCloud (US).

Configure the AWS WAF CloudFormation Stack Template

You can use these instructions to collect and send logs from a single **Web ACL**.

1. Login into the AWS console.
2. Go to the **CloudFormation** service.
3. Click **Create stack**.

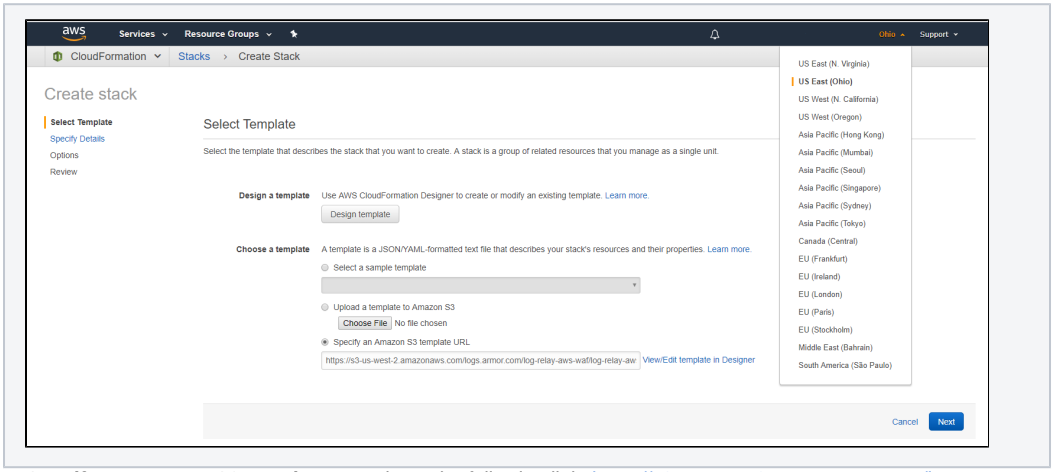
> AWS is in the process of updating the screens in their AWS console. As a result, there are two versions of the AWS CloudFormation screen.
>
> Review the following table to understand your particular view, and then review the appropriate option.

View	Sample image
Old View	
New View	

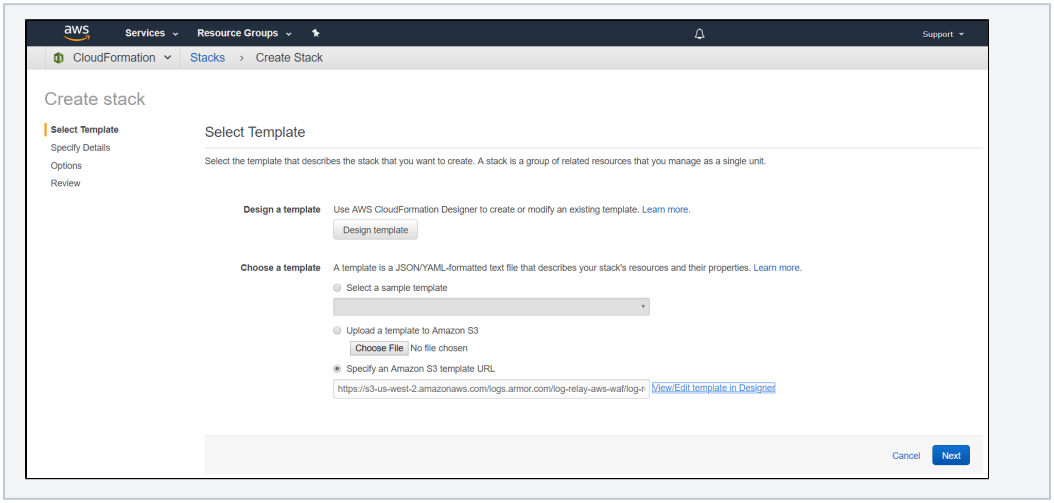
Option 1: Old View

1. In the AWS console, in the top menu, on the right side, select the desired region.

> ⚠ The CloudFormation template must be executed in the same region as the Web ACL.



2. In **Specify an Amazon S3 template URL**, input the following link: https://s3-us-west-2.amazonaws.com/logs.armor.com/log-relay-aws-waf/log-relay-aws-waf.yaml.



3. Click **Next**.
4. In **Stack name**, enter a descriptive name.
    - This name must begin with a letter, and can only contain letters, numbers, and hyphens.
5. In **ArmorLogEndpoint,** enter the URL (including protocol and port number) of the endpoint to which logs will be sent.
    - This is the IP address or DNS name of the log relay instance, using the https protocol and port 5443.
6. In **ArmorTenantId**, enter your Armor account number.
    a. This can be found in the **Account Overview** section of your AMP account.
7. In **BucketName**, enter your S3 bucket name. This must be globally unique.
    - This is the S3 bucket (name) created by the CloudFormation template.
8. In **BucketRetentionInDays**, enter the number of days logs are retained in the S3 bucket.
    a. By default, Armor has configured 3 days; set to 0 to keep logs until manually removed.
9. In **DeliveryStreamName**, enter the name of the Kinesis delivery stream for WAF logs.
    - This is the Kinesis stream created by the CloudFormation template.
    - The 'aws-waf-logs-' prefix will be added to the stream name.
10. In **StrictSsl**, indicate whether or not strict SSL checks should be enforced on the destination log URL (True or False).

> ⚠ Armor recommends that **StrictSsl** be set to True. Afterwards, you must complete the **steps to enable SSL** to utilize the CloudFormation template. If these steps are not performed, when you attempt to launch the newly created CloudFormation template, the process will fail.
>
> **Steps to enable SSL**
>
> **SSL/TLS Secured Communications**
>
> In most cases, we assume network isolation using subneting and/or firewalls are in place to secure communication between a log source and your Log Relay. There are a few exceptions to this assumption:

In scenarios where it is typical to have data traverse the Internet, or in scenarios where a device *only* supports TLS-secured transport, the Log Relay config supports TLS ingestion.

Certificates

When you install the Log Relay software, a self-signed certificate and its corresponding private key are generated and placed in **/opt/armor/logrelay.pem** and **/opt/armor/logrelay.key** respectively. If the device sending logs requires strict SSL checks, you have a few options to satisfy this requirement:

Exporting the Self-Signed Certificate

You may export the certificate and add it to the trust store of the log source device (if supported). You copy the PEM certificate from the Log Relay server and then consult the vendor-supplied documentation to install a new trusted certificate.

Using a Certificate from a Valid CA

You can also generate a CSR and request a certificate from a CA the log source device already trusts. Using openssl you can generate a new CSR. We recommend using a configuration file to supply Subject Alternate Names (SANs) for the various DNS hostnames pointed at your Log Relay in addition to its IP address.

logrealy.cnf

```
[ req ]
default_bits       = 2048
distinguished_name = req_distinguished_name
req_extensions     = req_ext

[ req_distinguished_name ]
countryName                = <COUNTRY>
stateOrProvinceName        = <STATE>
localityName               = <CITY>
organizationName           = <COMPANY_NAME>
commonName                 = <LOG_RELAY_IP_ADDRESS>

[ req_ext ]
subjectAltName = @alt_names

[alt_names]
DNS.1   = <DNS_NAME_1>
DNS.2   = <DNS_NAME_2>
DNS.3   = <DNS_NAME_3>
```

Fill in the values in angle brackets above with applicable values. For <**COUNTRY**> us the 2-digit ISO country code. For <**STATE**>. you can use the 2-digit abbreviation or the full name of your state or province.

If the IP address of the Log Relay changes frequently or you already use a DNS hostname as the *default* means of addressing the Log Relay, use the DNS hostname instead of the IP address in <**LOG_RELAY_IP_ADDRESS**>.

Add any DNS hostnames that resolve to this Log Relay using the **alt_names** section of the config. If you're not using any SANs, remove the [**alt_names**] and [**req_ext**] sections and remove the reference under the [**req**] section.

Then use **openssl** to request the certificate:

```
openssl req -new rsa:2048 -key /opt/armor/logrelay.key -nodes -out logrelay.csr -config
logrelay.cnf
```

Note that you may need to run this command as root as the key is owned by the Log Relay service account.

After you've generated your CSR and received the certificate from the CA, ensure that it is in PEM format and upload it to your Log Relay machine. Ensure that is accessible to the Log Relay service account.

Once the file is uploaded and has the correct permissions, update the override environment file to point at the path of the new certificate. Create a file at **/etc/sysconfig/armor-logstash.override** with the following contents:

```
ARMOR_LOGSTASH_SSL_CERT='/path/to/cert.pem'
```

If you used a key other than the one included with the Log Relay, you can specify it in this file as well:

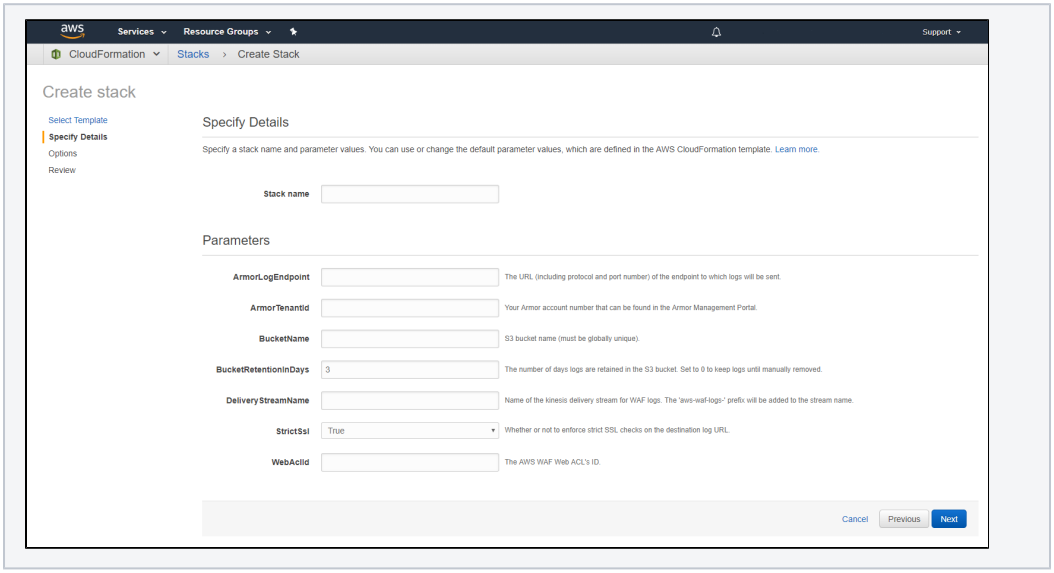
```
ARMOR_LOGSTASH_SSL_KEY='/path/to/private.key'
```

Note that this key must not have a password and be in PKCS8 format. You can use file permissions and/or selinux policies to protect the key.

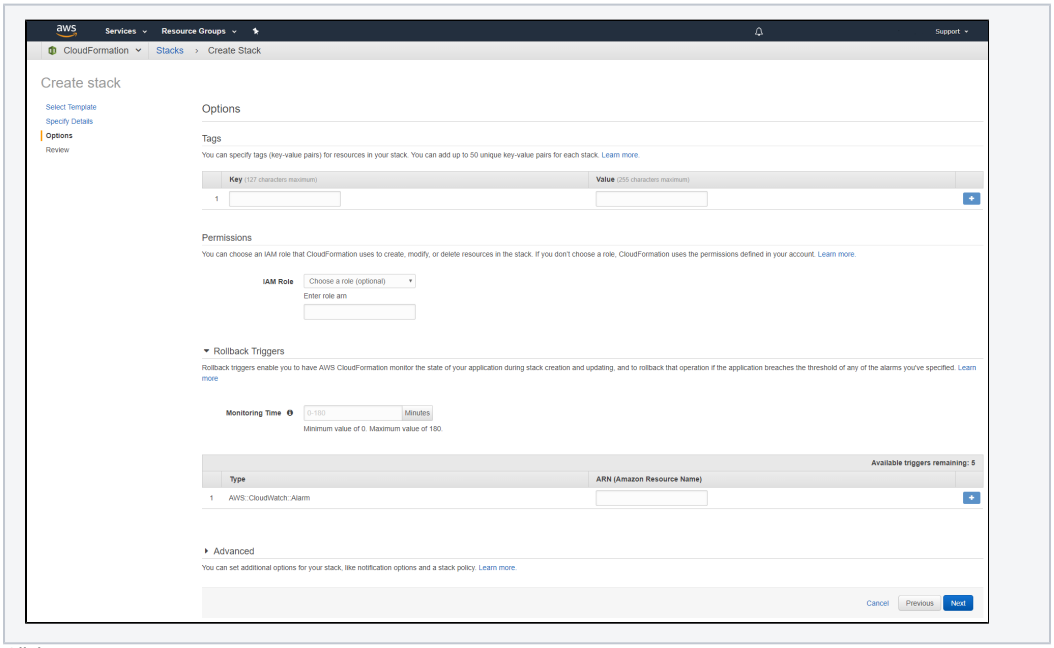
After creating or updating these configuration files, restart the Log Relay service:

```
sudo systemctl restart armor-logstash.service
```

11. In **WebAclId**, enter the ID of the AWS WAF Web ACL.



12. Click **Next**.
13. (Optional) If required by your organization, under **Tags**, add your organization's tags to the CloudFormation deployment.
14. (Optional) If required by your organization, under **Permissions**, in the drop-down menu, select **IAM role ARN**, and then in the corresponding field, enter **AWSCloudFormationStackSetExecutionRole**.

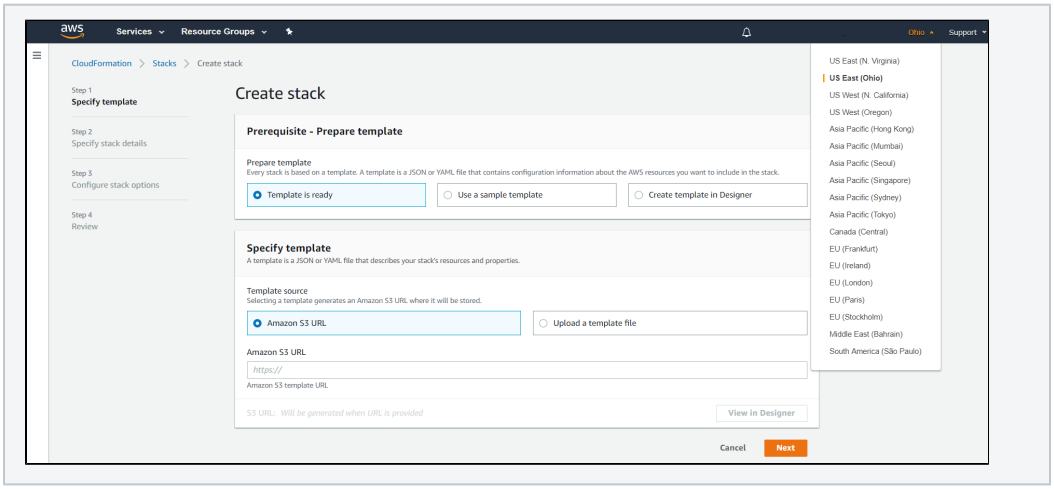


15. Click **Next**.
16. At the bottom of the screen, mark the box to accept the terms, and then click **Create**.

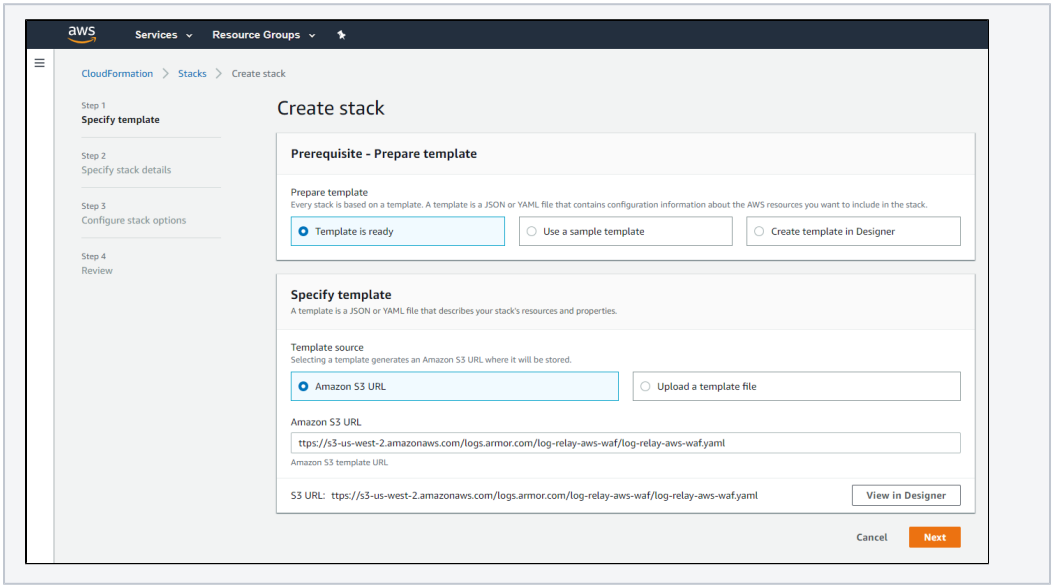
Option 2: New View

1. In the AWS console, in the top menu, on the right side, select the desired region for log collection.

> ⚠ The CloudFormation template must be executed in the same region as the Web ACL.



2. In **Amazon S3 URL**, input the following link: https://s3-us-west-2.amazonaws.com/logs.armor.com/log-relay-aws-waf/log-relay-aws-waf.yaml.



3. Click **Next**.
4. In **Stack name**, enter a descriptive name.
    - This name must begin with a letter, and can only contain letters, numbers, and hyphens.
5. In **ArmorLogEndpoint,** enter the URL (including protocol and port number) of the endpoint to which logs will be sent.
    - This is the IP address or DNS name of the log relay instance, using the https protocol and port 5443.
6. In **ArmorTenantId**, enter your Armor account number.
    a. This can be found in the **Account Overview** section of your AMP account.
7. In **BucketName**, enter your S3 bucket name. This must be globally unique.
    - This is the S3 bucket (name) created by the CloudFormation template.
8. In **BucketRetentionInDays**, enter the number of days logs are retained in the S3 bucket.
    a. By default, Armor has configured 3 days; set to 0 to keep logs until manually removed.
9. In **DeliveryStreamName**, enter the name of the Kinesis delivery stream for WAF logs.
    - This is the Kinesis stream created by the CloudFormation template.
    - The 'aws-waf-logs-' prefix will be added to the stream name.
10. In **StrictSsl**, indicate whether or not strict SSL checks should be enforced on the destination log URL (True or False).

> ⚠ Armor recommends that **StrictSsl** be set to True. Afterwards, you must complete the **steps to enable SSL** to utilize the CloudFormation template. If these steps are not performed, when you attempt to launch the newly created CloudFormation template, the process will fail.
>
> **Steps to enable SSL**

SSL/TLS Secured Communications

In most cases, we assume network isolation using subneting and/or firewalls are in place to secure communication between a log source and your Log Relay. There are a few exceptions to this assumption:

In scenarios where it is typical to have data traverse the Internet, or in scenarios where a device *only* supports TLS-secured transport, the Log Relay config supports TLS ingestion.

Certificates

When you install the Log Relay software, a self-signed certificate and its corresponding private key are generated and placed in **/opt/armor/logrelay.pem** and **/opt/armor/logrelay.key** respectively. If the device sending logs requires strict SSL checks, you have a few options to satisfy this requirement:

Exporting the Self-Signed Certificate

You may export the certificate and add it to the trust store of the log source device (if supported). You copy the PEM certificate from the Log Relay server and then consult the vendor-supplied documentation to install a new trusted certificate.

Using a Certificate from a Valid CA

You can also generate a CSR and request a certificate from a CA the log source device already trusts. Using openssl you can generate a new CSR. We recommend using a configuration file to supply Subject Alternate Names (SANs) for the various DNS hostnames pointed at your Log Relay in addition to its IP address.

logrealy.cnf

```
[ req ]
default_bits       = 2048
distinguished_name = req_distinguished_name
req_extensions     = req_ext

[ req_distinguished_name ]
countryName                = <COUNTRY>
stateOrProvinceName        = <STATE>
localityName               = <CITY>
organizationName           = <COMPANY_NAME>
commonName                 = <LOG_RELAY_IP_ADDRESS>

[ req_ext ]
subjectAltName = @alt_names

[alt_names]
DNS.1   = <DNS_NAME_1>
DNS.2   = <DNS_NAME_2>
DNS.3   = <DNS_NAME_3>
```

Fill in the values in angle brackets above with applicable values. For <**COUNTRY**> us the 2-digit ISO country code. For <**STATE**>. you can use the 2-digit abbreviation or the full name of your state or province.

If the IP address of the Log Relay changes frequently or you already use a DNS hostname as the *default* means of addressing the Log Relay, use the DNS hostname instead of the IP address in <**LOG_RELAY_IP_ADDRESS**>.

Add any DNS hostnames that resolve to this Log Relay using the **alt_names** section of the config. If you're not using any SANs, remove the [**alt_names**] and [**req_ext**] sections and remove the reference under the [**req**] section.

Then use **openssl** to request the certificate:

```
openssl req -new rsa:2048 -key /opt/armor/logrelay.key -nodes -out logrelay.csr -config
logrelay.cnf
```

Note that you may need to run this command as root as the key is owned by the Log Relay service account.

After you've generated your CSR and received the certificate from the CA, ensure that it is in PEM format and upload it to your Log Relay machine. Ensure that is accessible to the Log Relay service account.

Once the file is uploaded and has the correct permissions, update the override environment file to point at the path of the new certificate. Create a file at **/etc/sysconfig/armor-logstash.override** with the following contents:

```
ARMOR_LOGSTASH_SSL_CERT='/path/to/cert.pem'
```

If you used a key other than the one included with the Log Relay, you can specify it in this file as well:

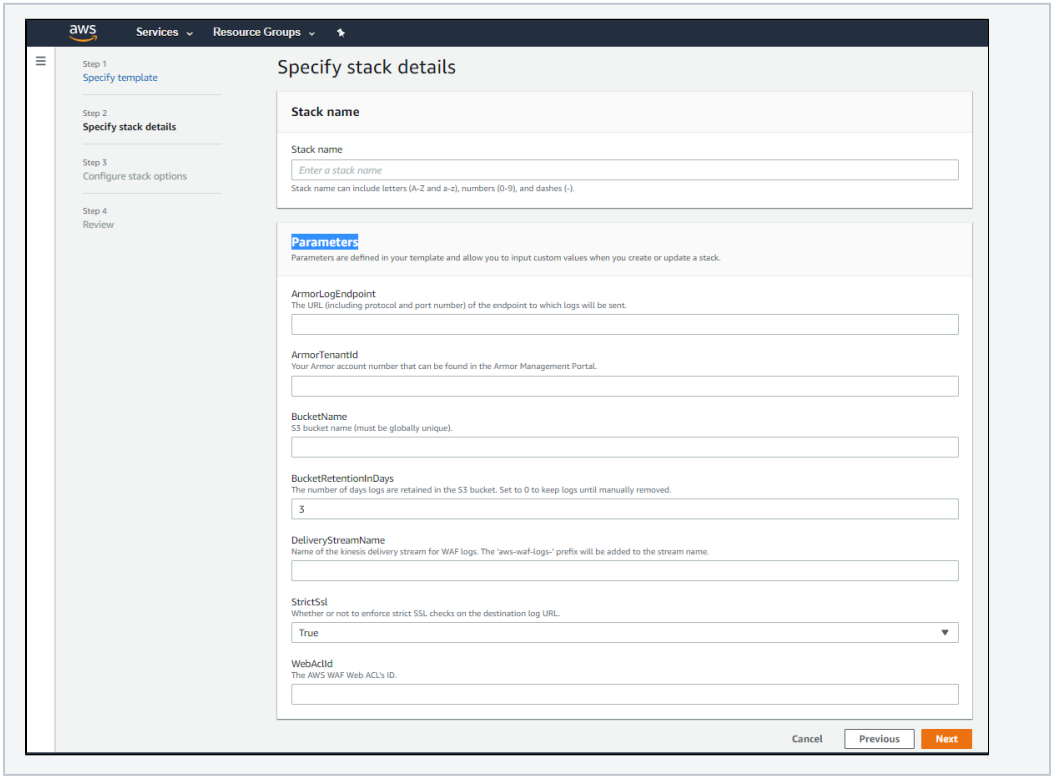
```
ARMOR_LOGSTASH_SSL_KEY='/path/to/private.key'
```

Note that this key must not have a password and be in PKCS8 format. You can use file permissions and/or selinux policies to protect the key.

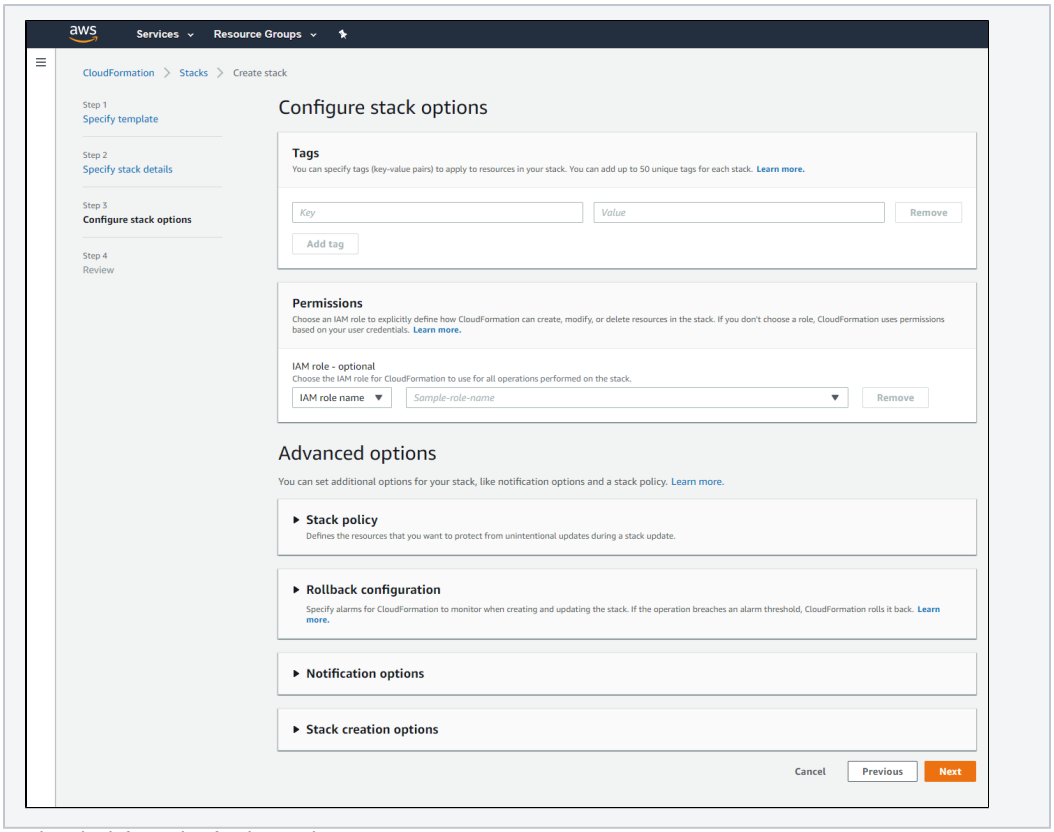
After creating or updating these configuration files, restart the Log Relay service:

```
sudo systemctl restart armor-logstash.service
```

11. In **WebAclId**, enter the ID of the AWS WAF Web ACL.



12. Click **Next**.
13. (Optional) If required by your organization, under **Tags**, add your organization's tags to the CloudFormation deployment.
14. (Optional) If required by your organization, under **Permissions**, in the drop-down menu, select **IAM role ARN**, and then in the corresponding field, enter **AWSCloudFormationStackSetExecutionRole**.

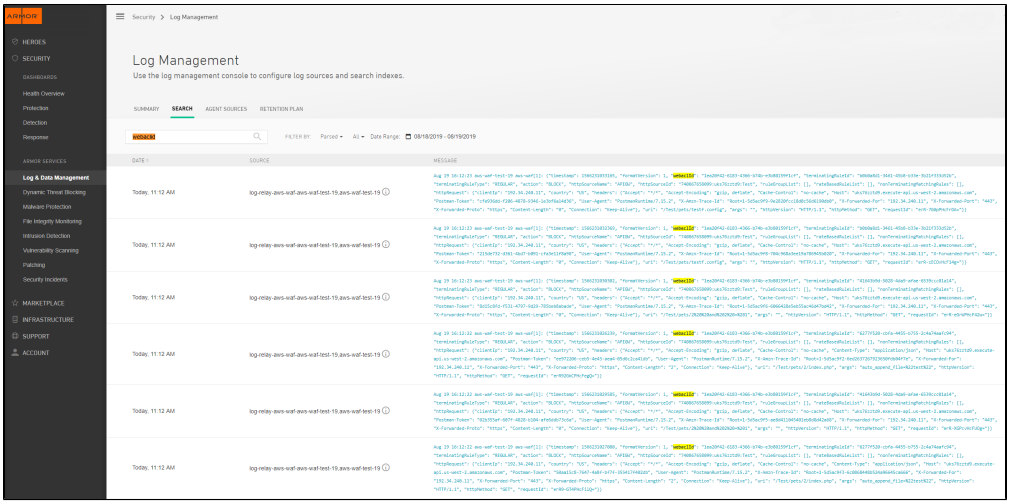


15. Review the information for the stack.
16. At the bottom of the screen, mark the box to accept the terms, and then click **Create stack**.

> ⚠ After a few minutes, the stack status should change from CREATE_IN_PROGRESS to CREATE_COMPLETE.

Verify Connection in AMP

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Security**.
2. Click **Log & Data Management**, and then select **Search**.
3. In the **Source** column, review the source name to locate the newly created AWS WAF remote log source.
    a. In the search field, you can also enter "webaclid" to locate AWS WAF messages.



Troubleshooting

If you are having issues adding a remote collector to an AWS WAF remote device, consider that:

- You do not have proper permissions in AWS.
- You entered the AWS account information for an incorrect AWS service account.
    - If you have multiple AWS accounts, especially child or organization accounts, you must verify that you added the service account information for the correct service account

Edit a Stack

This section only applies to single stacks, not stack sets.

Currently, Armor's AWS CloudFormation template does not support updates. If you want to update your stack, then you must delete the remote log source, and then create a new one with your desired updates.

Was this helpful?

Your Rating: Results: 7 rates