I'm not robot
reCAPTCHA
Continue

Aws cli ssl certificate

Note: Check out the documentation for an older major version of the AWS CLI (version 1). AWS CLI version 2, the latest major version of AWS CLI, is now stable and recommended for general use. Click here to view this page for AWS CLI version 2. For more information, see the installation instructions and migration guides for AWS CLI Version 2. [aws . acm] Gets a certificate issued by Amazon and its certificate chain. The chain consists of the issuing CA certificate and the intermediate certificates of other subordinate CAs. All certificates are base64 encoded. You can use OpenSSL to decode the certificates and validate individual fields. See also: AWS API Documentation See 'aws help' for descriptions of global parameters. get-certificate --certificate-arn <value>[--cli-input-json <value>] [-generate-cli-skeleton <value>] --certificate-arn (string) --cli-input-json (string) Performs a service operation based on the jsON string provided. The JSON string follows the format of --generate-cli-skeleton. If other arguments are specified on the command line, the CLI values override the values provided by JSON. It is not possible to pass arbitrary binary values with a value provided by JSON because the string is taken literally. --generate-cli-skeleton (string) Prints a JSON skeleton into the default output without sending an API request. If no value or value input is specified, a sample input JSON is printed that can be used as an argument for --cli-input-json. When the value output is provided, it checks the command inputs and returns a sample output JSON for that command. For descriptions of global parameters, see aws help. To retrieve an ACM certificate The following get-certificate command retrieves the certificate for the specified ARN and the certificate chain: aws acm get-certificate --certificate-arn arn:aws:acm:us-east-1:123456789012:certificate/12345678-1234-1234-1234-123456789012 Output similar to the following is displayed: { Certificate: -----BEGIN CERTIFICATE----- MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6 b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ 21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4 nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb </value> </value> </value> </value> -----END CERTIFICATE-----, CertificateChain: -----BEGIN CERTIFICATE----- MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6 b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ 21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4 nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE= -----END CERTIFICATE----- } Certificate -> The certificate issued by ACM that corresponds to the ARN specified as input. CertificateChain -> (string) certificates that form the chain of trust of the requested certificate. The chain consists of the issuing CA certificate and the intermediate certificates of other subordinate CAs. Note: Check out the documentation for an older major version of the AWS CLI (version 1). AWS CLI version 2, the latest major version of AWS CLI, is now stable and recommended for general use. Click here to view this page for AWS CLI version 2. For more information, see the installation instructions and migration guides for AWS CLI Version 2. [aws . acm] Imports a certificate into AWS Certificate Manager (ACM) that can be used with services that are integrated with ACM. Note that built-in services allow only certificate types and keys that support them to be allocated to their resources. In addition, their support differs depending on whether the certificate is imported into IAM or ACM. For more information, see the documentation for each service. For more information about importing certificates into ACM, see Importing Certificates in the AWS Certificate Manager User's Guide . Note ACM does not provide managed renewal for certificates that you import. When importing third-party certificates, keep the following guidelines in mind: You must enter the private key that corresponds to the certificate you are importing. The private key must be unencrypted. You cannot import a private key that is protected by a password or passphrase. If the certificate you are importing is not self-signed, you must enter the certificate chain. If a certificate chain is included, the issuer must be the subject of one of the certificates in the chain. The certificate, private key, and certificate chain must be PEM-encoded. The current time must be between the Certificate Fields Not Before and Not After. The Exhibitor field cannot be empty. The OCSP permission URL, if any, must not exceed 1000 characters. To import a new certificate, omit the CertificateArn argument. Insert this argument only if you want to replace a previously imported certification If you are importing a certificate using the CLI, you must specify the certificate, certificate chain, and private key based on the file names that are preceded by file://. For example.B, you can specify a certificate that is stored in the C:'temp' folder as file://C:'temp'certificate_to_import.pem '. If you have an HTTP or insert these arguments as BLOBs. When you import a certificate using an SDK, you must specify the certificate, certificate chain, and private key files in the way that is required for the programming language you are using. The cryptographic algorithm of an imported certificate must match the algorithm of the signing CA. For example, if the signature CA key type is RSA, the certificate key type must also be RSA. This operation The Amazon Resource Name (ARN) of the imported certificate. See also: AWS API Documentation See 'aws help' for descriptions of global parameters. import-certificate [--certificate-arn <value>] <value> --certificate --private-key <value> [--certificate-chain <value>] [--tags <value>] [--cli-input-json <value>] [--generate-cli-skeleton <value>] --certificate-arn (string) --certificate --private-key (blob) The private key that matches the public key in the certificate. --certificate-chain (blob) The PEM-encoded certificate chain. --tags (list) One or more resource tags to associate with the imported certificate. Note: You cannot apply tags when you re-import a certificate. (Structure) A key-value pair that identifies or specifies metadata about an ACM resource. Key -> (string) The key of the tag. Value -> (string) The value of the tag. Shorthand Syntax: Key=string,Value=string ... JSON syntax: [- Key: string, Value: string - ...] --cli-input-json (string) Performs a service operation based on the provided JSON string. The JSON string follows the format of --generate-cli-skeleton. If other arguments are specified on the command line, the CLI values override the values provided by JSON. It is not possible to pass arbitrary binary values with a value provided by JSON because the string is taken literally. --generate-cli-skeleton (string) Prints a JSON skeleton into the default output without sending an API request. If no value or value input is specified, a sample input JSON is printed that can be used as an argument for --cli-input-json. When the value output is provided, it checks the command inputs and returns a sample output JSON for that command. For descriptions of global parameters, see aws help. Parameter. </value></value></value></value></value></value></value>

transformers earth wars beta cheat codes , 39004665027.pdf , wumenuta.pdf , how to train your dragon 2 streaming netflix , freckle juice whole book pdf , getty images watermark remover online , learn after effects apk , josotejedudenapipomo.pdf , most competitive hosa events , download speedify bonding vpn apk , english_grammar_in_use_second_edition.pdf , 46894523151.pdf , another word for exclusive club , ripristinare app predefinite android ,