curl 60 ssl certificate problem

curl 60 ssl certificate problem is a common error encountered when using the cURL command-line tool or library to make HTTPS requests. This error indicates that cURL failed to verify the SSL certificate of the server it is trying to communicate with, which can lead to failed connections and security warnings. Understanding the underlying causes of this issue is crucial for developers, system administrators, and users who rely on secure data transfer over the internet. This article explores the common reasons behind the curl 60 ssl certificate problem, how SSL certificates work in this context, and practical methods to troubleshoot and resolve the error. Additionally, it covers best practices to maintain secure connections and avoid such SSL certificate issues in the future.

Understanding curl 60 SSL Certificate Problem

The **curl 60 ssl certificate problem** error occurs when cURL attempts to establish a secure HTTPS connection but cannot verify the server's SSL certificate. SSL certificates are digital credentials used to authenticate the identity of websites and encrypt data transmitted between a client and a server. When cURL cannot confirm the certificate's authenticity, it raises the curl error 60 to prevent potential security risks such as man-in-the-middle attacks. This error is part of cURL's internal error codes specifically related to SSL/TLS verification failures. The error message usually appears as "SSL certificate problem: unable to get local issuer certificate" or similar variations, indicating a failure in the certificate chain validation.

How SSL Certificates Work with cURL

When cURL connects to an HTTPS endpoint, it initiates an SSL/TLS handshake. During this handshake, the server presents its SSL certificate, which needs to be validated by the client (cURL). Validation involves checking that the certificate is issued by a trusted Certificate Authority (CA) and that the certificate chain is complete and unexpired. cURL uses a bundle of trusted CA certificates to verify the

server's certificate. If the certificate cannot be matched to a trusted CA or the chain is broken, cURL aborts the connection with the curl 60 error.

Significance of curl 60 in Secure Communications

The curl 60 error is critical because it signals a failure in ensuring the security and authenticity of the HTTPS connection. Ignoring this error can expose users to risks such as data interception or impersonation of trusted websites. Therefore, understanding and addressing curl 60 ssl certificate problem is essential for maintaining secure communication channels in applications, scripts, and network tools that utilize cURL.

Common Causes of curl 60 SSL Certificate Problem

Several factors can trigger the curl 60 ssl certificate problem, ranging from server-side issues to client-side configuration problems. Identifying the root cause is vital for effective troubleshooting and resolution.

Missing or Outdated CA Certificates

One of the most frequent causes of curl 60 errors is the absence or outdated state of the CA certificate bundle on the client machine. cURL relies on this bundle to verify the authenticity of SSL certificates. If the CA certificates are missing, expired, or not updated, cURL will fail to validate the server's certificate.

Self-Signed or Invalid Server Certificates

Servers using self-signed certificates or certificates that are not recognized by trusted CAs will cause cURL to report a curl 60 ssl certificate problem. These certificates lack a valid trust chain, making them untrusted by default.

Intermediate Certificate Issues

Improper server configuration that omits intermediate certificates in the SSL chain can cause validation failures. Even if the server certificate is valid, missing intermediates prevent cURL from verifying the full certificate chain.

Expired or Revoked Certificates

Certificates that have expired or been revoked by their issuing authority will not pass validation checks. cURL will detect these conditions and raise the curl 60 error accordingly.

Incorrect System Date and Time

If the client system's clock is set incorrectly, SSL certificate validation may fail since certificates are only valid within specific date ranges. An inaccurate system time can trigger curl 60 errors.

Network Interception or Proxy Issues

In some environments, proxies or network security appliances intercept SSL traffic and present their own certificates. Without proper configuration, cURL may reject these certificates, leading to the curl 60 ssl certificate problem.

Diagnosing the SSL Certificate Verification Failure

Accurate diagnosis of the curl 60 ssl certificate problem involves examining the error messages generated by cURL and inspecting the SSL certificate chain.

Reviewing cURL Error Messages

cURL typically outputs detailed error messages when it encounters a problem. The error message associated with curl 60 often includes descriptions such as "unable to get local issuer certificate" or "certificate verify failed." These messages hint at missing CA certificates or broken certificate chains.

Using Verbose Mode for Detailed Debugging

Running cURL with the *-v* or *--verbose* flag provides detailed output of the SSL handshake and certificate verification process. This verbose output reveals the certificates presented, the verification steps, and where the failure occurs, aiding in pinpointing the exact issue.

Checking the CA Certificate Bundle

Verifying the presence and integrity of the CA certificate bundle used by cURL is essential. The location of this bundle varies depending on the operating system and cURL installation. Checking its existence and updating it to the latest version often resolves verification failures.

Inspecting Server Certificate Chain

Analyzing the server's SSL certificate chain using external tools or online SSL checkers can reveal missing

intermediate certificates or other configuration errors on the server side that cause the curl 60 error.

Solutions and Workarounds for curl 60 SSL Certificate Problem

Several methods can resolve the curl 60 ssl certificate problem depending on its cause. These solutions range from updating certificates to modifying cURL's behavior.

Updating CA Certificate Bundle

Ensuring the CA certificate bundle is current is one of the most effective solutions. This can be done by:

- Installing or updating the *ca-certificates* package on Linux distributions.
- Downloading the latest CA bundle from trusted sources and configuring cURL to use it.
- Ensuring the operating system's root certificates are up to date.

Specifying the CA Bundle Manually

Using the *--cacert* option, users can specify a custom CA certificate file for cURL to use during SSL verification. This is useful when working with private CAs or self-signed certificates.

Disabling SSL Verification (Not Recommended)

As a last resort, the *--insecure* or *-k* option disables SSL certificate verification in cURL. Although this bypasses the curl 60 error, it exposes the connection to security risks and should be avoided in production environments.

Configuring Server to Serve Complete Certificate Chain

For server administrators, ensuring the server is configured to present the full certificate chain, including intermediate certificates, is vital. This prevents clients like cURL from encountering verification errors.

Correcting System Date and Time

Verifying and setting the correct system date and time on the client machine can eliminate curl 60 errors caused by invalid certificate validity periods.

Handling Proxy and Network Interception

Configuring cURL to trust proxy certificates or disabling interception in network appliances can resolve SSL verification failures when proxies are involved. Adding the proxy's CA certificate to the trusted bundle may be necessary.

Best Practices for Managing SSL Certificates with cURL

Proper management of SSL certificates and cURL configuration ensures secure and reliable HTTPS communication without encountering curl 60 ssl certificate problem.

Regularly Update CA Certificates

Maintaining up-to-date CA certificates on client systems and servers is fundamental. Automated updates and monitoring for certificate expiration help prevent verification failures.

Use Valid and Trusted Server Certificates

Deploy SSL certificates issued by reputable Certificate Authorities and ensure the complete certificate chain is correctly installed on servers.

Avoid Disabling SSL Verification

Disabling SSL verification should be avoided except in controlled testing environments. Always prefer fixing the root cause of the curl 60 error to maintain security.

Implement Logging and Monitoring

Enable logging for cURL operations and monitor SSL-related errors to proactively address issues before they impact users or applications.

Educate Teams on SSL and cURL Usage

Providing training and documentation on SSL certificate management and cURL usage helps reduce configuration mistakes that lead to curl 60 errors.

Frequently Asked Questions

What does 'curl 60 SSL certificate problem' mean?

The 'curl 60 SSL certificate problem' indicates that cURL failed to verify the SSL certificate of the server. This usually happens because the certificate is invalid, expired, self-signed, or the CA bundle on your system is outdated or missing.

How can I fix the 'curl 60 SSL certificate problem'?

To fix this error, you can update your system's CA certificates, specify the correct certificate bundle with the --cacert option, or temporarily bypass certificate verification with the -k or --insecure flag (not recommended for production).

Why does cURL fail SSL verification on some websites but not others?

cURL may fail SSL verification if the website uses a certificate signed by an unknown or untrusted Certificate Authority (CA), or if your local CA bundle is outdated and does not include the CA that signed the website's certificate.

Is it safe to use the --insecure flag to bypass curl SSL certificate errors?

Using the --insecure flag disables SSL certificate verification, which can expose you to man-in-the-middle attacks. It should only be used temporarily for testing or in controlled environments, not for production or sensitive data transfers.

How do I update the CA certificates to resolve curl 60 errors on Ubuntu?

On Ubuntu, you can update CA certificates by running: sudo apt-get update && sudo apt-get install --reinstall ca-certificates. This ensures your system's CA bundle is up-to-date and trusted by cURL.

Can a self-signed SSL certificate cause the curl 60 error?

Yes, self-signed certificates are not trusted by default and will cause cURL to fail SSL verification with error 60 unless you explicitly trust the certificate or disable verification.

How to specify a custom CA certificate file in cURL to fix error 60?

You can specify a custom CA certificate file using the --cacert option in cURL, for example: curl --cacert /path/to/ca-bundle.crt https://example.com. This tells cURL to use the provided certificate bundle for verification.

What role does the CURLOPT_CAINFO option play in fixing curl 60 SSL errors in code?

CURLOPT_CAINFO allows you to specify the path to a CA certificate bundle in your cURL code. Setting this option to a valid CA bundle helps cURL verify SSL certificates correctly and avoid error 60.

Additional Resources

1. *Mastering cURL: Troubleshooting SSL Certificate Issues*
This book dives deep into the world of cURL, focusing specifically on common SSL certificate problems including the infamous "curl 60" error. It guides readers through understanding SSL/TLS protocols, certificate validation, and how to debug and resolve certificate trust issues. Practical examples and step-by-step instructions make it suitable for developers and system administrators alike.

2. *SSL Certificates and cURL: A Developer's Guide*
A comprehensive guide that explains the interaction between SSL certificates and cURL requests. It covers certificate authorities, self-signed certificates, and how to configure cURL to handle various SSL certificate scenarios. The book also addresses security best practices to ensure safe and reliable HTTP communications.

3. *HTTP and SSL: Solving cURL Error 60 and Beyond*
Focused on HTTP communications secured by SSL/TLS, this book tackles the "curl 60" SSL certificate problem head-on. It offers detailed explanations of certificate validation processes, common pitfalls, and practical troubleshooting techniques. Readers will learn how to verify certificates, update CA bundles, and configure their environments properly.

4. *Practical SSL for Developers: Managing Certificates with cURL*
This book provides a hands-on approach to managing SSL certificates within development workflows using cURL. It explains the importance of trusted certificate stores, how to handle expired or misconfigured certificates, and tools to diagnose SSL connection errors. The content is enriched with real-world scenarios and solutions.

5. *Debugging SSL Errors in cURL: A Technical Handbook*
A technical manual aimed at developers and IT professionals facing SSL errors when using cURL. The book breaks down error codes, including the notorious error 60, and provides detailed methodologies to diagnose and fix these issues. It also covers environment-specific considerations such as operating system differences and proxy configurations.

6. *Secure Communications with cURL and SSL Certificates*
This title explores the principles of establishing secure communications using cURL alongside SSL certificates. It explains certificate chains, root and intermediate certificates, and how cURL validates these during HTTPS requests. Readers gain practical knowledge on configuring cURL options to circumvent or properly handle SSL certificate errors.

7. *Understanding SSL Certificate Validation Errors in cURL*
A focused study on SSL certificate validation errors encountered by cURL users, including error 60. The book provides insights into how certificate authorities work, why certificates may fail validation, and the implications of bypassing these checks. It emphasizes security implications and best practices for maintaining trust.

8. *cURL for Web Developers: Handling SSL and Security Challenges*
Designed for web developers, this book addresses common SSL-related challenges when using cURL for API calls and web requests. It covers the setup of trusted certificate stores, handling self-signed certificates, and troubleshooting connection errors. The guide also includes tips to improve security without compromising functionality.

9. *SSL Troubleshooting Essentials: From Certificate Issues to cURL Fixes*
A concise resource for troubleshooting SSL issues, this book covers a range of problems including the cURL 60 error. It offers practical advice on updating CA certificates, verifying server certificates, and configuring client-side SSL options. The book is ideal for anyone needing quick, effective solutions to SSL-related connectivity problems.

Curl 60 Ssl Certificate Problem

curl 60 ssl certificate problem: Networking and Kubernetes James Strong, Vallery Lancey, 2021-09-08 Kubernetes has become an essential part of the daily work for most system, network, and cluster administrators today. But to work effectively together on a production-scale Kubernetes system, they must be able to speak the same language. This book provides a clear guide to the layers of complexity and abstraction that come with running a Kubernetes network. Authors James Strong and Vallery Lancey bring you up to speed on the intricacies that Kubernetes has to offer for large container deployments. If you're to be effective in troubleshooting and maintaining a production cluster, you need to be well versed in the abstraction provided at each layer. This practical book shows you how. Learn the Kubernetes networking model Choose the best interface for your clusters from the CNCF Container Network Interface project Explore the networking and Linux primitives that power Kubernetes Quickly troubleshoot networking issues and prevent downtime Examine

cloud networking and Kubernetes using the three major providers: Amazon Web Services, Google Cloud, and Microsoft Azure Learn the pros and cons of various network tools--and how to select the best ones for your stack

curl 60 ssl certificate problem: Web Security Testing Cookbook Paco Hope, Ben Walther, 2008-10-14 Offering developers an inexpensive way to include testing as part of the development cycle, this cookbook features scores of recipes for testing Web applications, from relatively simple solutions to complex ones that combine several solutions.

curl 60 ssl certificate problem: Practical Go Amit Saha, 2021-09-11 YOUR PRACTICAL, HANDS-ON GUIDE TO WRITING APPLICATIONS USING GO Google announced the Go programming language to the public in 2009, with the version 1.0 release announced in 2012. Since its announcement to the community, and the compatibility promise of the 1.0 release, the Go language has been used to write scalable and high-impact software programs ranging from command-line applications and critical infrastructure tools to large-scale distributed systems. It’s speed, simplicity, and reliability make it a perfect choice for developers working in various domains. In Practical Go - Building Scalable Network + Non-Network Applications, you will learn to use the Go programming language to build robust, production-ready software applications. You will learn just enough to building command line tools and applications communicating over HTTP and gRPC. This practical guide will cover: Writing command line applications Writing a HTTP services and clients Writing RPC services and clients using gRPC Writing middleware for network clients and servers Storing data in cloud object stores and SQL databases Testing your applications using idiomatic techniques Adding observability to your applications Managing configuration data from your applications You will learn to implement best practices using hands-on examples written with modern practices in mind. With its focus on using the standard library packages as far as possible, Practical Go will give you a solid foundation for developing large applications using Go leveraging the best of the language’s ecosystem.

curl 60 ssl certificate problem: Cloud Native Go Matthew A. Titmus, 2024-10-14 Learn how to use Go's strengths to develop services that are scalable and resilient even in an unpredictable environment. With this book's expanded second edition, Go developers will explore the composition and construction of cloud native applications, from lower-level Go features and mid-level patterns to high-level architectural considerations. Each chapter in this new edition builds on the lessons of the previous chapter, taking intermediate to advanced developers through Go to construct a simple but fully featured distributed key-value store. You'll learn about Go generics, dependability and reliability, memory leaks, and message-oriented middleware. New chapters on security and distributed state delve into critical aspects of developing secure distributed cloud native applications. With this book you will: Learn the features that make Go an ideal language for building cloud native software Understand how Go solves the challenges of designing scalable distributed services Design and implement a reliable cloud native service by leveraging Go's lower-level features such as channels and goroutines Apply patterns, abstractions, and tooling to effectively build and manage complex distributed systems Overcome stumbling blocks when using Go to build and manage a cloud native service

curl 60 ssl certificate problem: Kubernetes in Action Marko Luksa, 2017-12-14 Summary Kubernetes in Action is a comprehensive guide to effectively developing and running applications in a Kubernetes environment. Before diving into Kubernetes, the book gives an overview of container technologies like Docker, including how to build containers, so that even readers who haven't used these technologies before can get up and running. Purchase of the print book includes a free eBook in PDF, Kindle, and ePub formats from Manning Publications. About the Technology Kubernetes is Greek for helmsman, your guide through unknown waters. The Kubernetes container orchestration system safely manages the structure and flow of a distributed application, organizing containers and services for maximum efficiency. Kubernetes serves as an operating system for your clusters, eliminating the need to factor the underlying network and server infrastructure into your designs. About the Book Kubernetes in Action teaches you to use Kubernetes to deploy container-based

distributed applications. You'll start with an overview of Docker and Kubernetes before building your first Kubernetes cluster. You'll gradually expand your initial application, adding features and deepening your knowledge of Kubernetes architecture and operation. As you navigate this comprehensive guide, you'll explore high-value topics like monitoring, tuning, and scaling. What's Inside Kubernetes' internals Deploying containers across a cluster Securing clusters Updating applications with zero downtime About the Reader Written for intermediate software developers with little or no familiarity with Docker or container orchestration systems. About the Author Marko Luksa is an engineer at Red Hat working on Kubernetes and OpenShift. Table of Contents PART 1 - OVERVIEW Introducing Kubernetes First steps with Docker and Kubernetes PART 2 - CORE CONCEPTS Pods: running containers in Kubernetes Replication and other controllers: deploying managed pods Services: enabling clients to discover and talk to pods Volumes: attaching disk storage to containers ConfigMaps and Secrets: configuring applications Accessing pod metadata and other resources from applications Deployments: updating applications declaratively StatefulSets: deploying replicated stateful applications PART 3 - BEYOND THE BASICS Understanding Kubernetes internals Securing the Kubernetes API server Securing cluster nodes and the network Managing pods' computational resources Automatic scaling of pods and cluster nodes Advanced scheduling Best practices for developing apps Extending Kubernetes

curl 60 ssl certificate problem: Containers for Developers Handbook Francisco Javier Ramírez Urea, 2023-11-28 Effortlessly create and manage complex multi-component applications based on Docker containers Key Features Gain a clear understanding of software containers from the SecDevOps perspective Master the construction of application pieces within containers to achieve a seamless life cycle Prepare your applications to run smoothly and with ease in complex container orchestrators Purchase of the print or Kindle book includes a free PDF eBook Book DescriptionDevelopers are changing their deployment artifacts from application binaries to container images, giving rise to the need to build container-based apps as part of their new development workflow. Managing an app’s life cycle is complex and requires effort—this book will show you how to efficiently develop, share, and execute applications. You’ll learn how to automate the build and delivery process using CI/CD tools with containers as container orchestrators manage the complexity of running cluster-wide applications, creating infrastructure abstraction layers, while your applications run with high availability, resilience, and persistence. As you advance, you’ll develop, test, and debug applications on your desktop and get them ready to run in production with optimal security standards, using deployment patterns and monitoring tools to help identify common issues. You’ll also review deployment patterns that’ll enable you to solve common deployment problems, providing high availability, scalability, and security to your applications. Finally, you’ll explore different solutions to monitor, log, and instrument your applications as per open-source community standards. By the end of this book, you’ll be able to manage your app’s life cycle by implementing CI/CD workflows using containers to automate the building and delivery of its components.What you will learn Find out how to build microservices-based applications using containers Deploy your processes within containers using Docker features Orchestrate multi-component applications on standalone servers Deploy applications cluster-wide in container orchestrators Solve common deployment problems such as persistency or app exposure using best practices Review your application’s health and debug it using open-source tools Discover how to orchestrate CI/CD workflows using containers Who this book is forThis book is for developers and DevOps engineers looking to learn about the implementation of containers in application development, especially DevOps engineers who deploy, monitor, and maintain container-based applications running on orchestrated platforms. In general, this book is for IT professionals who want to understand Docker container-based applications and their deployment. A basic understanding of coding and frontend-backend architectures is needed to follow the examples presented in this book.

curl 60 ssl certificate problem: Troubleshooting Puppet Thomas Uphill, 2015-08-31 Troubleshoot your Puppet infrastructure to leverage your system's performance effectively About

This Book Covers major tools in Puppet deployment Fix catalog compilation problems and deal with issues found in larger deployments, such as scaling and improving performance. A fast-paced guide with real-world examples Who This Book Is For If you are a beginner to intermediate Puppet Engineer looking for guidance to help fix problems with your Puppet deployments, this book is for you. What You Will Learn Debug your Puppet infrastructure Use APIs to ensure services are working properly Fix catalog compilation issues Solve problems using Hiera tool Detect problems in your environment using PuppetDB tool Learn ways to format code to aid in identifying errors Troubleshoot errors in modules and templates In Detail Puppet is a configuration management system written for system administrators to manage a large number of systems efficiently and help maintain order. Deploying Puppet becomes more complex as you increase the number of nodes in your environment. The Puppet tool is an intelligent solution that increases the automation footprint for the proactive management of server infrastructures. Puppet's simple programming language is usable on most operating systems and is portable on different deployment environments. We begin by looking at the puppet.conf server configuration file, and talk about possible problems that can occur. What does puppet really do in the background and what options does it provide for troubleshooting? This is what we will explore. Moving on, we will be troubleshooting errors made in modules and templates, finding the best solutions. We will be writing code that will helping us in identify errors. Then we will explain how several ENCs do their job and how puppet communicates with them. We will learn how PuppetDB collects data generated by Puppet. It also enables advanced Puppet features like exported resources, and can be the foundation for other applications that use Puppet's data. By the end of the book we will have learned the best debugging tips for Puppet and PuppetServer. Style and approach This is a quick-paced guide packed with real-world examples and solutions to obstacles in your Puppet infrastructure.

curl 60 ssl certificate problem: Kubernetesトラブルシューティングガイド 桐井 祐樹, 小沢 周平, 2023-03-10 本書は日々クラウドのトラブルシューティングに携わる筆者が、Kubernetesで起こりうるトラブル事例をまとめ、Kubernetesのトラブル事例の要因と対処方法を紹介した解説書です。トラブル事例ごとに豊富なコマンド例を掲載し、エラーメッセージの読み解き方と対処方法を身につけられる内容となっています。特定のクラウドサービス固有のトラブルシューティングではなく、Kubernetesそのものが持つ機能や出力されるメッセージを活用して、各種トラブルへ対処する事例を紹介します。そのため、クラスターが動作しているクラウド環境にかかわらず参考にしていただける一冊です。【目次】第1章 Kubernetesの基本コマンドと調査ツール 第2章 アプリケーションPodのトラブルシューティング 第3章 ネットワークのトラブルシューティング 第4章 ストレージのトラブルシューティング 第5章 Kubernetesクラスター/ノードのトラブルシューティング 付録A 困ったときは - オンラインの情報源とコミュニティー

curl 60 ssl certificate problem: La sicurezza dellle applicazioni Web. Tecniche di testing e prevenzione Paco Hope, Ben Walther, 2009

curl 60 ssl certificate problem: *Kubernetes* Serena Sensini, 2023-05-24T00:00:00+02:00 Kubernetes è un software open-source di orchestrazione e gestione di container che ha rivoluzionato il modo in cui le applicazioni vengono costruite, distribuite e conservate. Sviluppato da Google, oggi è mantenuto da Cloud Native Computing Foundation ed è in grado di lavorare con sistemi diversi, tra cui Docker. Dopo un'introduzione ai container, il manuale passa a illustrare le caratteristiche di Kubernetes, la sua architettura, le funzioni di base per lo sviluppo e i concetti chiave di master, node, pod e service. Si passa poi ad approfondire l'uso integrato con altri software, come Docker, le funzioni avanzate, come l'autoscaling, per arrivare alle potenzialità di distribuzione sulle piattaforme cloud AWS, Azure e Google. Ricca di istruzioni passo passo e di esempi, questa guida è adatta a tutti gli sviluppatori che vogliono imparare a sfruttare la potenza di Kubernetes per gestire applicazioni su larga scala in maniera agile, affidabile ed efficiente.

curl 60 ssl certificate problem: Kubernetes в действии Марко Лукша, 2022-01-29 Книга детально рассказывает о Kubernetes – открытом программном обеспечении Google для автоматизации развёртывания, масштабирования и управления приложениями. Поддерживает основные технологии контейнеризации, также возможна поддержка технологий аппаратной виртуализации. Дано пошаговое разъяснение принципов работы и устройства модулей фреймворка. Вы узнаете все о создании объектов верхнего уровня, развертывании кластера на собственной рабочей машине и построении федеративного кластера в нескольких дата-центрах. Также детально проанализированы задачи обеспечения безопасности в

Kubernetes.Издание будет интересно всем, для кого актуальны проблемы организации кластеров и автоматизации развёртывания, масштабирования и управления приложениями.

curl 60 ssl certificate problem: *Apache Security* Ivan Ristic, 2005 The complete guide to securing your Apache web server--Cover.

curl 60 ssl certificate problem: Billboard , 1959-06-08 In its 114th year, Billboard remains the world's premier weekly music publication and a diverse digital, events, brand, content and data licensing platform. Billboard publishes the most trusted charts and offers unrivaled reporting about the latest music, video, gaming, media, digital and mobile entertainment issues and trends.

Related to curl 60 ssl certificate problem

What is the meaning of "curl -k -i -X" in Linux? When you use curl to access a web page it is actually sending the GET request to the server. There are other kinds of request that can be used and -X is the way to specify this.

bash - Curl bad URL (3) - Unix & Linux Stack Exchange Both the above scripts concatenates all files given as arguments on the command line, and passes the output to curl, one line at a time. Note that I have also corrected the HTTP

How to fix curl sslv3 alert handshake failure? - Unix & Linux Stack How do I ignore or force the certificate using curl command line? When using wget seems to work fine. Also works when testing with openssl as below: $ openssl s_client -connect

How to send multiline data in curl body within bash script? I am trying to send multi-line comment in the curl body from bash script. Below is my curl invocation. #!/bin/bash temp="This is sample data: 2019/05/21 03:33:04 This is 2nd

How to trust self-signed certificate in cURL command line? 1 If you save off the self-signed.crt from your server, you can pass it to curl via "--cacert self-signed.crt" and curl will validate the certificate of your server using the given CA Cert

502 Bad Gateway when curl is talking to API A curl command in a Bash script (called by cron) asks a web service/API, on another device/server (hosts both the API and the SQL database), to perform an operation on

curl - Adding a self-signed certificate to the "trusted list" - Unix I've generated a self-signed certificate for my build server and I'd like to globally trust the certificate on my machine, as I created the key myself and I'm sick of seeing warnings. I'm on

How to use curl -w option to redirect the output to a different file How to use curl -w option to redirect the output to a different file descriptor from stdout to avoid appending it at the end of curl response? Ask Question Asked 3 years ago

Why my curl gets stuck at getting anything from some domains? The curl command inside WSL2 hangs for some domains (like youtube.com) and it runs well for other domains (like google.com). It turns out the reason is the MTU size gap

CURL request using .netrc file - Unix & Linux Stack Exchange 15 As I understand the man page (of curl), the option -n just enables looking for a .netrc file, but it does not expect the file path of this file. This is the option --netrc-file. From the

What is the meaning of "curl -k -i -X" in Linux? When you use curl to access a web page it is actually sending the GET request to the server. There are other kinds of request that can be used and -X is the way to specify this.

bash - Curl bad URL (3) - Unix & Linux Stack Exchange Both the above scripts concatenates all files given as arguments on the command line, and passes the output to curl, one line at a time. Note that I have also corrected the HTTP

How to fix curl sslv3 alert handshake failure? - Unix & Linux Stack How do I ignore or force the certificate using curl command line? When using wget seems to work fine. Also works when testing with openssl as below: $ openssl s_client -connect

How to send multiline data in curl body within bash script? I am trying to send multi-line comment in the curl body from bash script. Below is my curl invocation. #!/bin/bash

temp="This is sample data: 2019/05/21 03:33:04 This is 2nd

How to trust self-signed certificate in cURL command line? 1 If you save off the self-signed.crt from your server, you can pass it to curl via "--cacert self-signed.crt" and curl will validate the certificate of your server using the given CA Cert

502 Bad Gateway when curl is talking to API A curl command in a Bash script (called by cron) asks a web service/API, on another device/server (hosts both the API and the SQL database), to perform an operation on

curl - Adding a self-signed certificate to the "trusted list" - Unix I've generated a self-signed certificate for my build server and I'd like to globally trust the certificate on my machine, as I created the key myself and I'm sick of seeing warnings. I'm on

How to use curl -w option to redirect the output to a different file How to use curl -w option to redirect the output to a different file descriptor from stdout to avoid appending it at the end of curl response? Ask Question Asked 3 years ago

Why my curl gets stuck at getting anything from some domains? The curl command inside WSL2 hangs for some domains (like youtube.com) and it runs well for other domains (like google.com). It turns out the reason is the MTU size gap

CURL request using .netrc file - Unix & Linux Stack Exchange 15 As I understand the man page (of curl), the option -n just enables looking for a .netrc file, but it does not expect the file path of this file. This is the option --netrc-file. From the

Back to Home: https://staging.massdevelopment.com