Umbrella Reporting API über Postman verwenden

Inhalt

Einleitung

In diesem Dokument wird die Verwendung der Cisco Umbrella Reporting-API in Postman beschrieben.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Cisco Umbrella.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Überblick

Die Umbrella API wurde im September 2022 veröffentlicht und bietet eine benutzerfreundliche und sichere Plattform, mit der Benutzer auf Umbrella aufbauen, diese erweitern und integrieren können.

Die Umbrella-API-Endpunkte werden auf api.umbrella.com gehostet und enthalten gruppierte

Pfade für jeden Anwendungsfall. API-Schlüssel können sowohl im Umbrella Dashboard unter Admin > API-Schlüssel als auch programmgesteuert mit der KeyAdmin-API verwaltet werden. Jeder Schlüssel kann mit mehreren Bereichen präzise konfiguriert werden, die in fünf primären Anwendungsfällen gruppiert sind:

- Mit Admin-API-Endpunkten können Sie Umbrella-API-Schlüssel und -Benutzer bereitstellen und verwalten, Rollen anzeigen und Kunden für Anbieter und verwaltete Anbieter verwalten.
- Über Auth-API-Endpunkte können Sie die Integration anderer Services in die Umbrella-Plattform autorisieren.
- API-Endpunkte für Bereitstellungen ermöglichen die Bereitstellung, Überwachung und Verwaltung von Netzwerken und anderen Einheiten sowie deren Sicherung, indem sie in Ihren vorhandenen Umbrella-Richtlinien konfiguriert werden.
- Mit Richtlinien-API-Endpunkten können Sie Ziellisten und die Ziele pro Liste bereitstellen und verwalten.
- Berichte über API-Endpunkte ermöglichen das Lesen und Überprüfen von Echtzeit-Sicherheitsinformationen zu Ihren Bereitstellungen. Die Umbrella App Discovery API bietet Einblicke in Ihre Cloud-basierten Anwendungen.

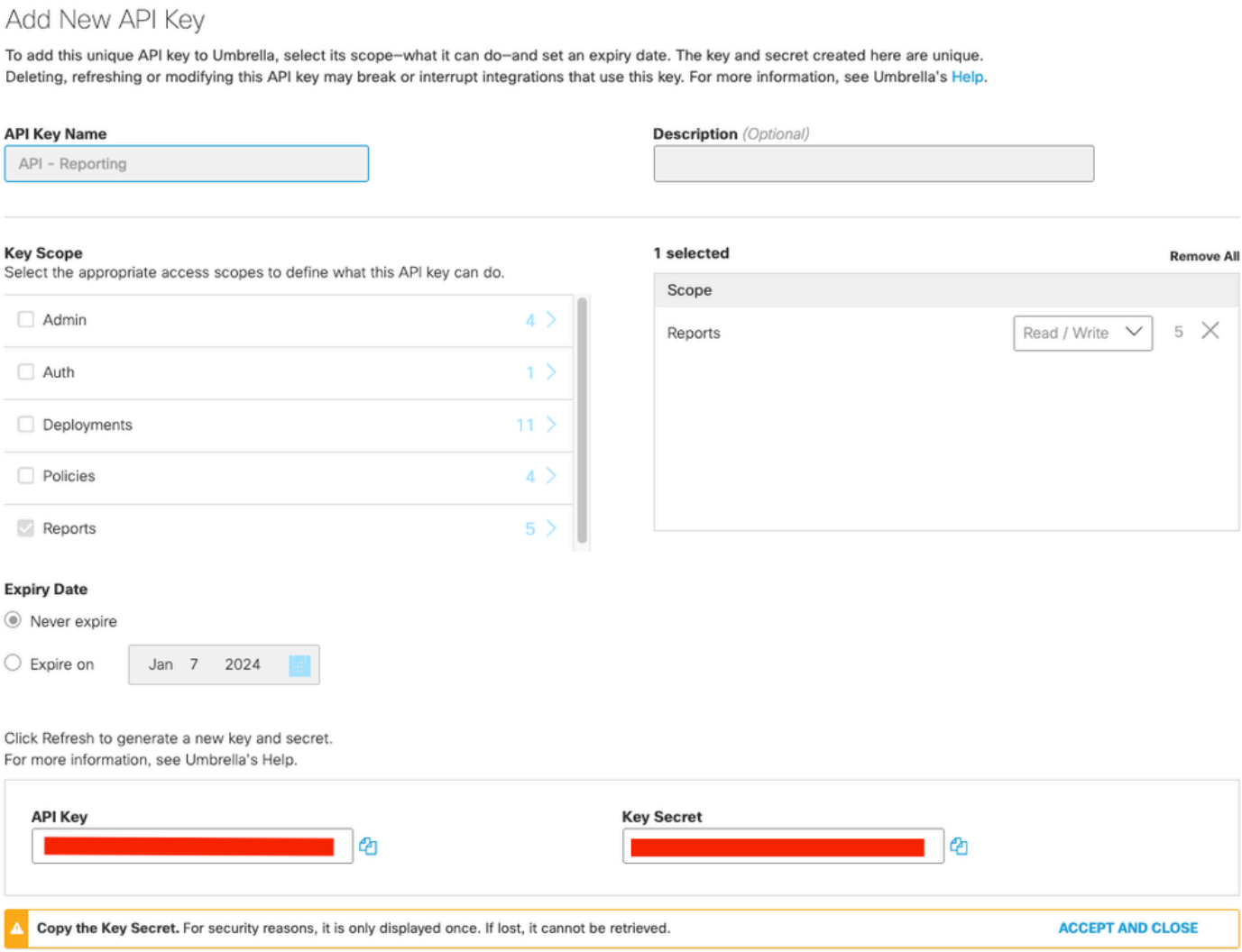
In diesem Artikel wird veranschaulicht, wie Aktivitätssuchberichte über die API gesammelt werden.

Rahmenverfahren

1. Navigieren Sie im Umbrella Dashboard zu Admin > API Keys.

2. Wählen Sie API Keys > Add.

3. Wählen Sie unter Schlüsselbereich die Option Berichte und dann Schlüssel erstellen.



21495050167956

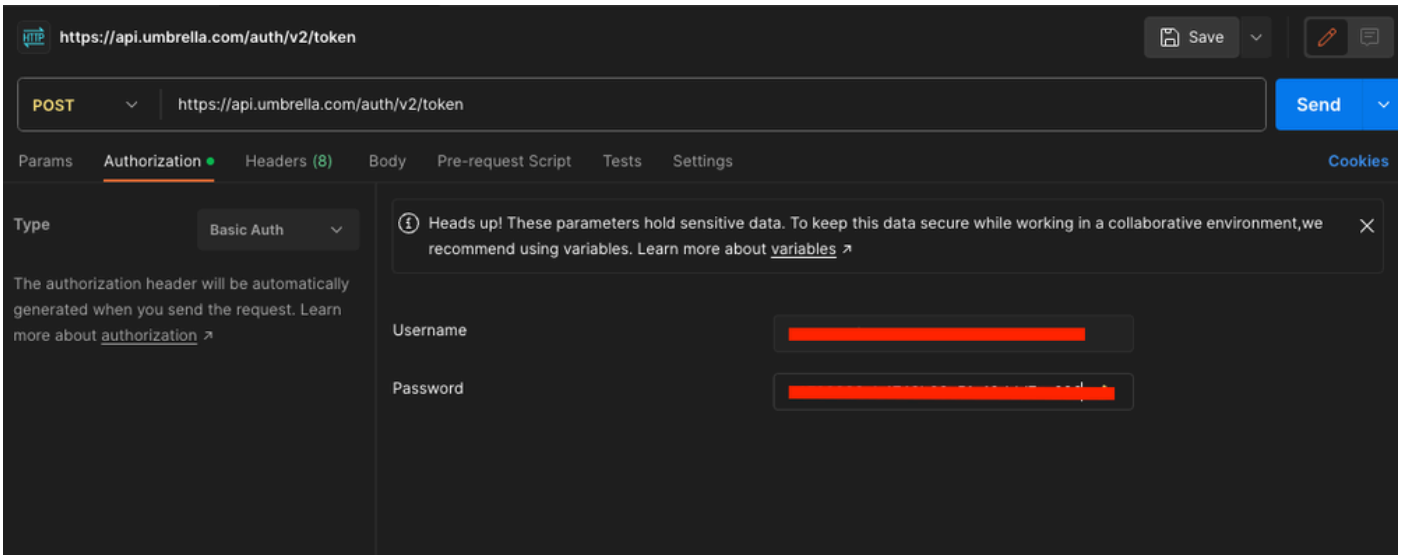
Administratoren können die Zugriffsebene pro Bereich zwischen Lesen/Schreiben und Nur-Lesen je nach der beabsichtigten Verwendung der einzelnen API-Schlüssel anpassen, während die API-Schlüssel so konfiguriert werden können, dass sie an einem vordefinierten Datum ablaufen. Sie müssen in diesem Schritt den API-Schlüssel/Schlüssel erfassen, da diese derzeit sichtbar sind und nicht danach angezeigt werden können.

Die API-Anmeldeinformationen generieren API-Zugriffstoken, die 60 Minuten lang gültig sind. Dieses Verfahren unterstützt den OAuth 2.0-Clientanmeldeinformationsfluss. In Umbrella-Umgebungen mit mehreren Organisationen oder in Service-Provider-Umgebungen können über die API-Anmeldeinformationen der übergeordneten Organisation Zugriffstoken mit denselben Gültigkeitsbereichen für eine untergeordnete Organisation generiert werden, die während des Autorisierungsprozesses angegeben wurde.

Postverfahren

Zunächst müssen Sie ein OAuth 2.0-Zugriffstoken erstellen. Die Umbrella-API-Authentifizierungspfade beginnen mit https://api.umbrella.com/auth/v2. Nach dem Einreichen einer POST-Abfrage und eines Benutzer-API-Schlüssels als Benutzername und API-Kennwort wird ein

Zugriffs-Token generiert.

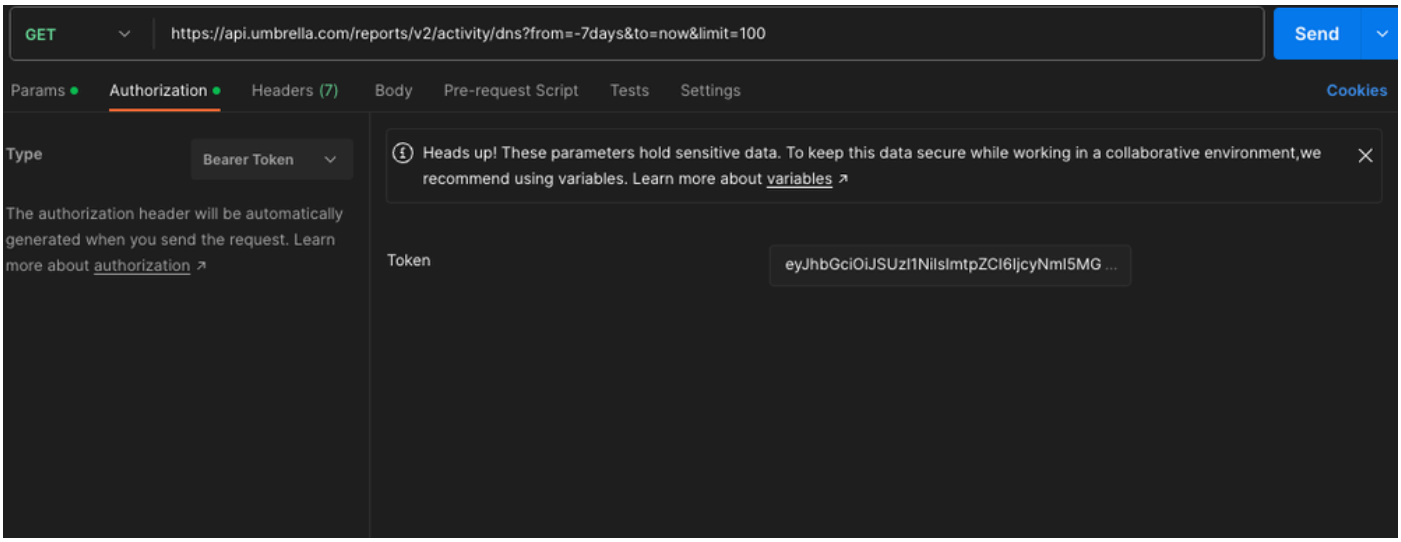


21606708808468

21607051456276

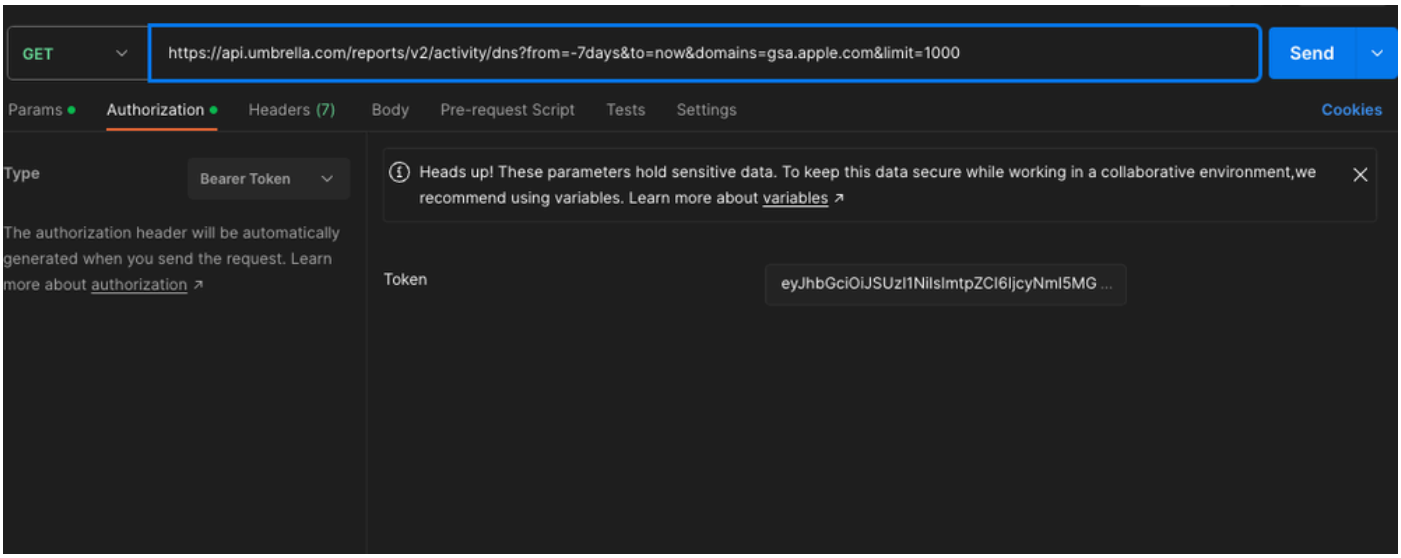
In diesem Schritt müssen Sie das Zugriffstoken sammeln. Jetzt können Sie Informationen mit dem Zugriffstoken abrufen.

Sie müssen die GET-Methode auswählen und sowohl den API-Pfad (einschließlich des erforderlichen Parameters) als auch das Zugriffs-Token eingeben. In diesem Beispiel können Sie 100 Berichte aus der Aktivitätssuche für die letzten 7 Tage ausschließlich nach DNS-Datenverkehr abrufen.



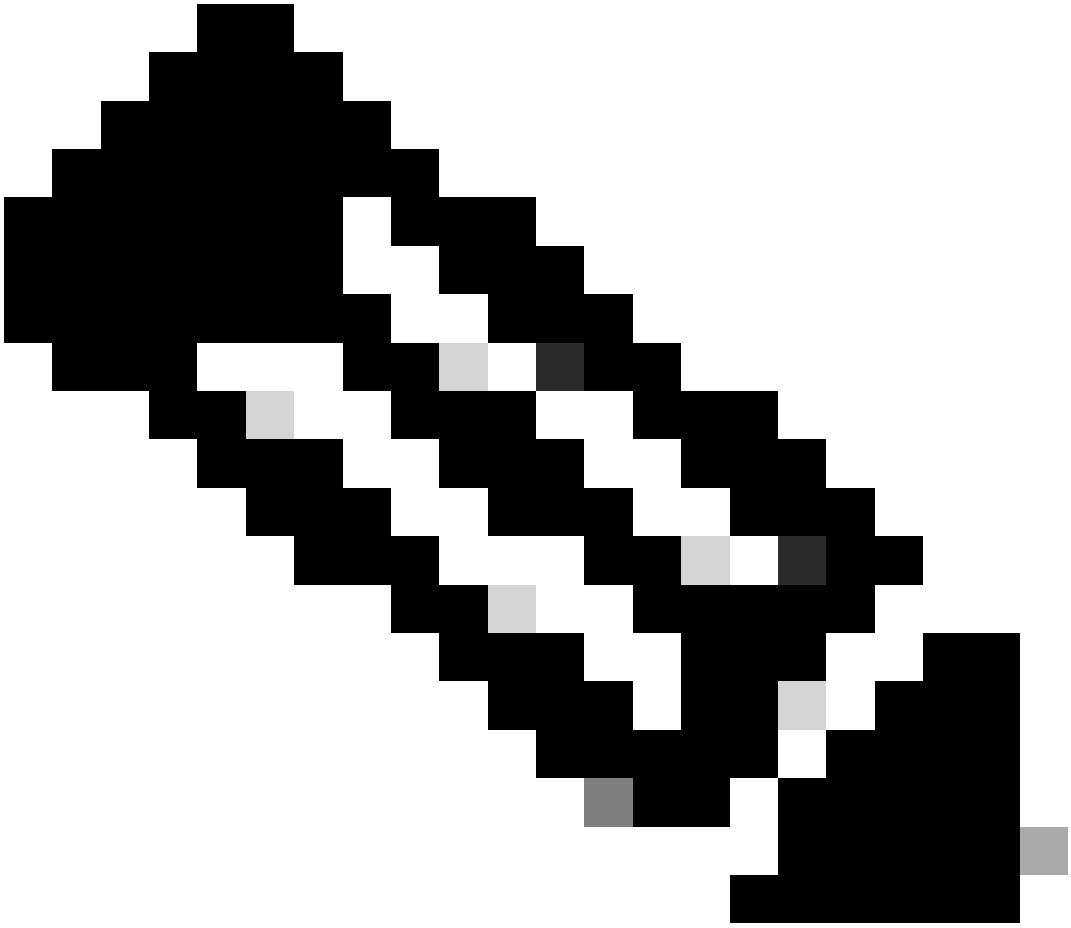
21607952074772

In einem anderen Beispiel können Sie versuchen, 1000 Berichte aus der Aktivitätssuche zu extrahieren, die ausschließlich für den DNS-Datenverkehr der letzten 7 Tage verwendet wurden, insbesondere für die Domäne "gsa.apple.com".



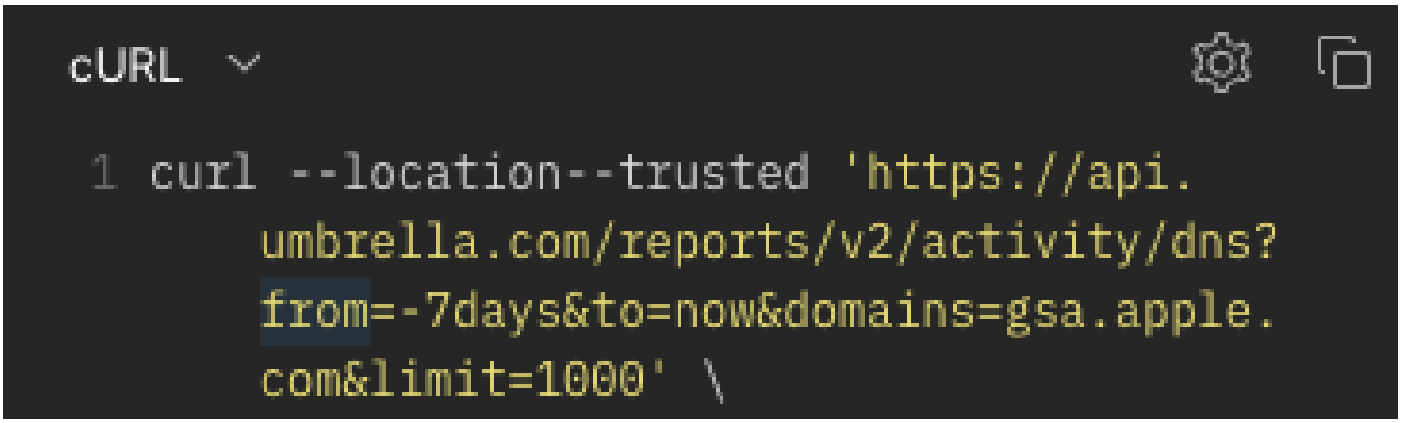
21607927544468

Unter Abfrageparameter anfordern können Sie weitere Parameter ermitteln, die Sie in Ihrer API-Abfrage verwenden können.



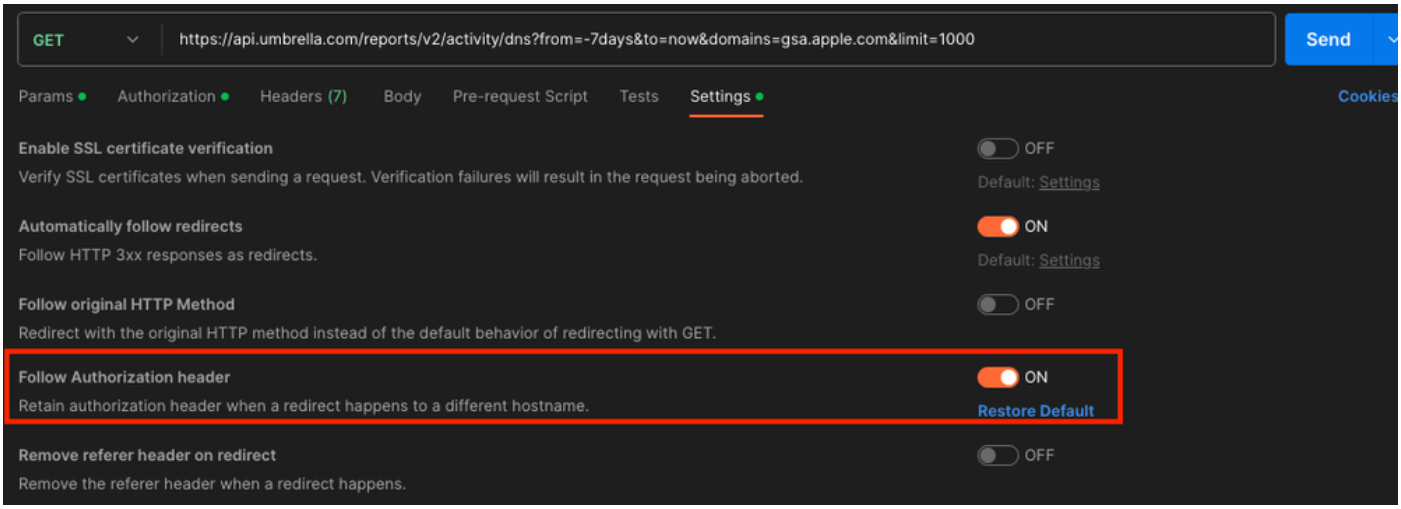
Anmerkung: Wenn eine HTTP-Client-Anfrage nicht von demselben Kontinent ausgeht wie der Standort des Umbrella Data Warehouse, antwortet der Umbrella-Server mit 302 Found (Gefunden). Um HTTP-Anfragen automatisch umzuleiten und den HTTP-Autorisierungsheader beizubehalten, können Sie zusätzliche Flags festlegen oder eine Umleitungseinstellung aktivieren.

Locke: Sie müssen die Flags -L oder —location und —location-trusted übergeben, um die HTTP-Curl-Anforderung umzuleiten und den Autorisierungs-Header beizubehalten.



21608126036628

Postbote: Navigieren Sie in der Postman-Umgebung zu einer API, und wählen Sie eine GET-Methode aus. Navigieren Sie zu Settings > Enable Follow Authorization-Header, um den Autorisierungs-Header für Umleitungsanforderungen beizubehalten.



21608126042388

Antworten

Nachdem Sie die GET-Aktion an die URL gesendet haben, können Sie verschiedene Statuscodes erhalten:

- Status: 200: Die angeforderten Informationen wurden erfolgreich verarbeitet.
- Status: 400: Ungültige Anforderung. Sie kann sich auf die URL beziehen, die Sie zur Abfrage gesendet haben. Ein oder mehrere Parameter sind falsch.
- Status: 401: Nicht autorisiert. Der Autorisierungsheader fehlt oder das Token ist nicht autorisiert.
- Status: 403: Verboten. Das Token ist ungültig.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.