SIEM Log Pull Admin Guide

Cloudbrink's Log Pull feature enables the ability to continuously send logs from the Cloudbrink Admin Portal, into customer hosted SIEM log servers.

Cloudbrink provides customers with centralized visibility and management control. Customers can define all their policies from a single cloud-based management console. Similarly, customers can view all the data about their users, endpoints and apps from the single console even though users are accessing all types of apps – SaaS, public/private cloud hosted apps and on-prem datacentre hosted apps.

This guide outlines the process for configuring the Log Pull feature to effectively send logs to your preferred SIEM Log Server.

Introduction

This document will walkthrough how to configure logs from the Cloudbrink admin portal to be sent to a customers SIEM log server.

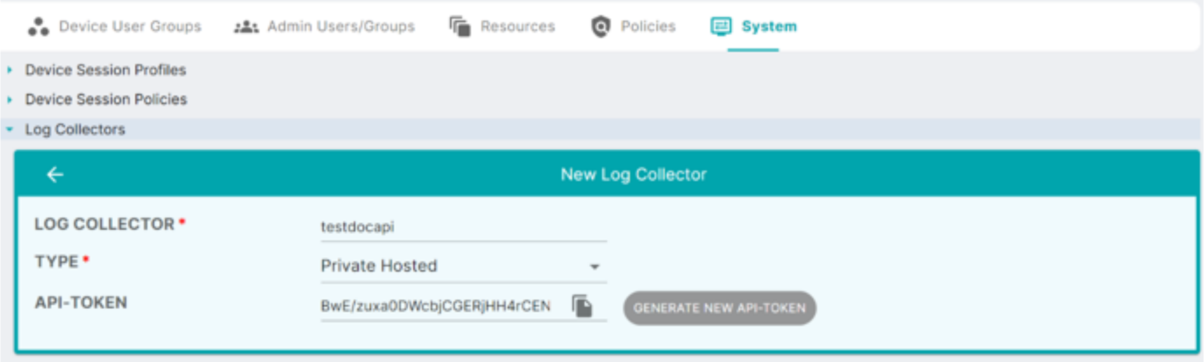
Prerequisites

- Cloudbrink admin portal access
- SIEM server deployed
- Scripting API client to authenticate, then retrieve log messages

SIEM Log Pull Config

1. When logging into the Cloudbrink Admin Portal, navigate to > Configure > System > Log Collectors > **New Log Collector.**

2. Add a new Log Collector by providing a name to the log collector entity, setting TYPE to “**Private Hosted**” by default, and click "**Generate new api-token**"



LOG COLLECTOR * testdocapi

TYPE * Private Hosted

API-TOKEN BwE/zuxa0DWcbjCGERjHH4rCEN

SIEM Log Pull Config - Continued

1. Create a client side script to call the log-retrieve API using the above token. Any scripting language that can call RESTful API's may be utilized.
2. Get an access token from the API-Token. Note, each {customer-ORG-code} is unique. If you are unsure what the ORG code is, reach out to support@cloudbrink.com.

```
curl --request GET \
  --url 'https://wren.cloudbrink.com/v2/providers/clb/orgs/{customer-ORG-code}/auth/access-token?valid_mins=60' \
  --header 'Content-Type: application/json' \
  --header 'x-cb-api-refresh: BQE6qfEUr9/
```

3. The response to the above request will contain the access-token in the response body

```
"BgGm/dWRFAfv43iPUfJGzaH8QhtLAFR9SKPbe32qGvtXKS1doDkyWVr3uUCVxEBfafprfO44v5kYhBZjaPYWs2JEvOICC8KKeLgbX/upMy9psvvwFb2PdNkwl5yB9qhQ3sjJseam1bW0fDpifMd8jpOrf4/TPKZLKkY9u/m7rvI5ejR4Icw+KEsO72hoV7TBBsPXAI1qDeU7rp8NgwunECxfSzCtc9vzmGVYV1gHxaKajRHDvVcBwwsQDF1yTOm2HWyAvuES69/FzTEZYHLpBH17AR3jkxsjuKJJk1HYI6XdLSPn1YdBy4A/1uInRQeYwCIaJilYrAa06TwfguZYOQ9SBx4gCZho+vosHlBoDJVDFzlwzexcjMfal1f+NTRkPvxPOZh8hTilxm1Z0oFnOyKV5tkk105AzFUVKKqT5NZiFxkumCS6sPGrb9+X5ivZzBNtBgpsmvNNEmlmX7hFr4PYvVqfo+Br/u1wQOKXuFs+DoZdUQRjVkEf0mzcZgsR0XA3SzoPSyajCOy6RMc="
```

4. Retrieve log data using the above access token.

```
curl --request GET \
  --url 'https://wren.cloudbrink.com/apis/siem-proxy/v1.0/providers/CLB/orgs/{customer-ORG-code}/logs?cont_token=640bdb3a70e11bda24c8c95e&limit=1000' \
  --header 'Authorization: BgGm/dWRFAfv43iPUfJGzaH8QhtLAFR9SKPbe32qGvtXKS1doDkyWVr3uUCVxEBfafprfO44v5kYhBZjaPYWs2JEvOICC8KKeLgbX/upMy9psvvwFb2PdNkwl5yB9qhQ3sjJseam1bW0fDpifMd8jpOrf4/TPKZLKkY9u/m7rvI5ejR4Icw+KEsO72hoV7TBBsPXAI1qDeU7rp8NgwunECxfSzCtc9vzmGVYV1gHxaKajRHDvVcBwwsQDF1yTOm2HWyAvuES69/FzTEZYHLpBH17AR3jkxsjuKJJk1HYI6XdLSPn1YdBy4A/1uInRQeYwCIaJilYrAa06TwfguZYOQ9SBx4gCZho+vosHlBoDJVDFzlwzexcjMfal1f+NTRkPvxPOZh8hTilxm1Z0oFnOyKV5tkk105AzFUVKKqT5NZiFxkumCS6sPGrb9+X5ivZzBNtBgpsmvNNEmlmX7hFr4PYvVqfo+Br/u1wQOKXuFs+DoZdUQRjVkEf0mzcZgsR0XA3SzoPSyajCOy6RMc=' \
  --header 'accept: application/json'
```

SIEM Log Pull Config - Continued

5. The response body to the above request contains the log data from Cloudbrink

```
[
    {
            "log_level": "AUDIT",
            "message": "Access Token validation successful",
            "message_timestamp": "2023-03-11T01:37:11.129Z"
    },
    {
            "log_level": "AUDIT",
            "message": "Access Token validation successful",
            "message_timestamp": "2023-03-11T01:37:36.361Z"
    }
]
```

6. When the access-token expires, the API-token can be used as per step-1 and get the new access-token. Repeat steps to regenerate the token.
7. **Note:** Customers can delete an existing API-token client from the management portal. Once deleted, any existing scripts using the API-client token will stop receiving the responses