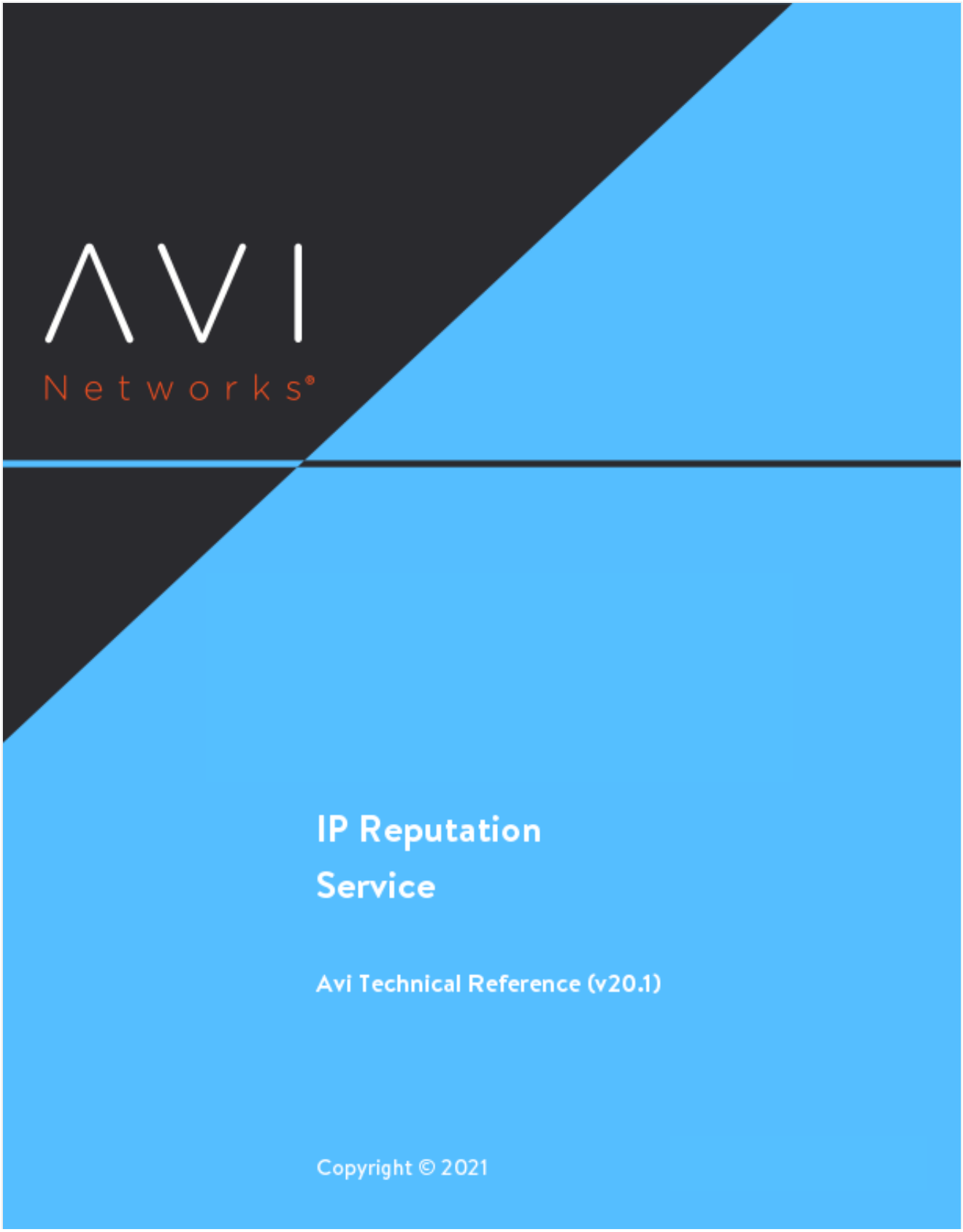


IP Reputation Service

Avi Technical Reference (v20.1)

IP Reputation Service

view online

Overview

This guide explains the IP reputation service of Avi Pulse.

With globally distributed Avi Controller clusters and with an ever changing landscape of insecure IP addresses, it is extremely channeling to maintain a real-time, up-to-date, consistent security posture across the Avi Controllers.

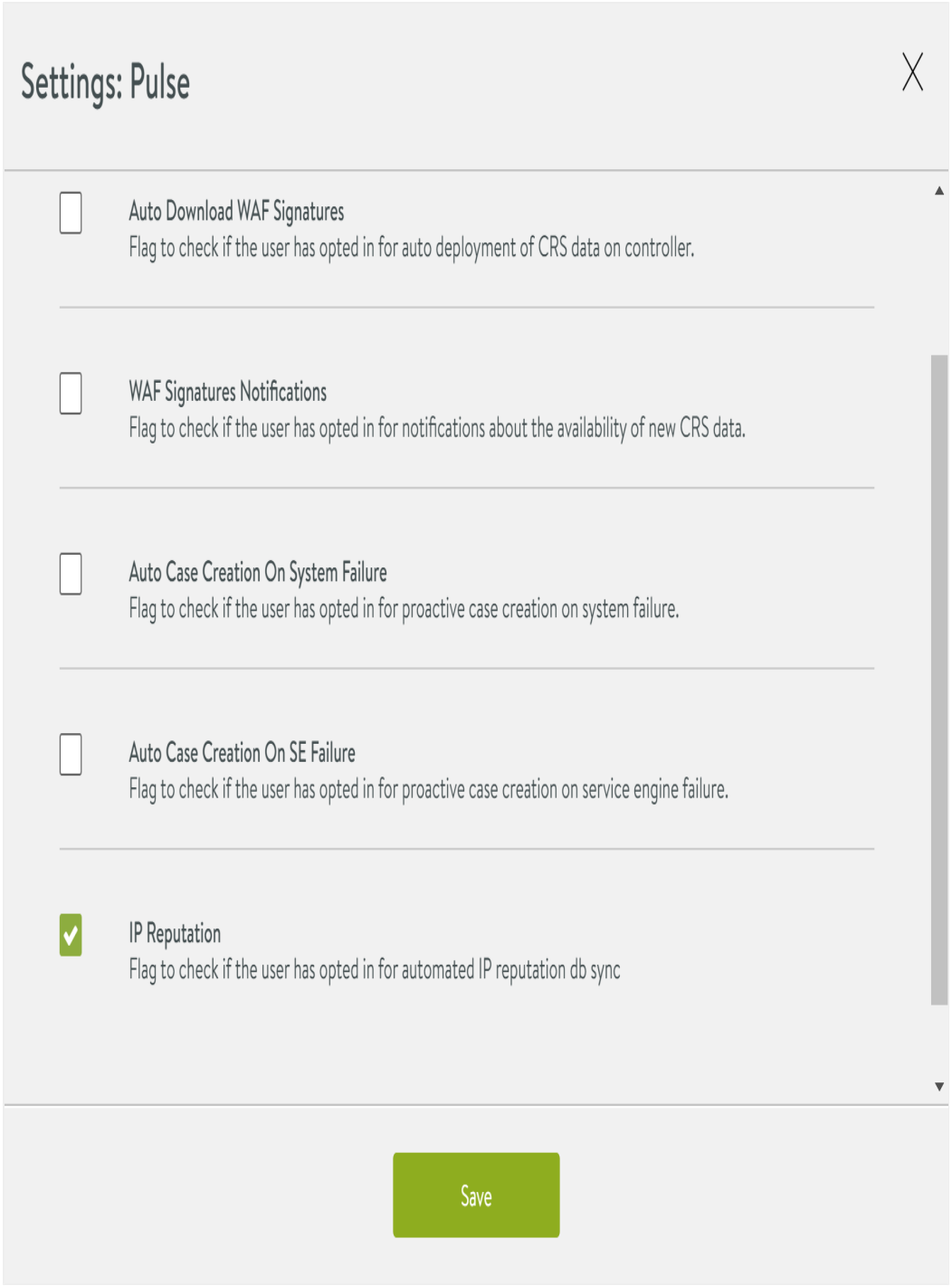
Avi Pulse's IP Reputation security threat intelligence service solves this for the customers by providing a real-time feed of updated IP scores.

IP Reputation Service

IP Reputation Service is part of the Avi Pulse service, and it is not enabled by default on Avi Controller. Avi Pulse is a centralized API gateway for the Controllers to consume different services from Avi Vantage/VMware. Avi Pulse provides advanced support, security, and licensing services to the Avi deployments. These are optional services that customers can enable on their accounts and the Controllers.

IP Reputation service polls the NSC WebRoot cache every five minutes for the database information. IP reputation service blocks all kinds of threats associated with the particular IP address and blocks malicious IP addresses, in-real time. The IP reputation database is available almost dynamically (every five minutes).

You can enable the IP Reputation service on an Avi Controller by checking IP Reputation option in opt-in options.



IP Reputation Database

The IP Reputation service enables the Avi Controller to sync with the IP Reputation Database provider or vendor. Avi Vantage uses WebRoot as the service provider for providing the IP Reputation databases.

The IP Reputation service filters out the relevant data from the raw data received from the NCS WebRoot cache server. WebRoot publishes the IP Reputation database in the form of text files.

Each Avi Controller cluster pulls the database through the Pulse service and updates all Service Engines as part of the normal configuration process.

WebRoot publishes the new IP reputation database every day. In addition to that, there are updates to the database published every few minutes.

The database consists of the following two types of files: * The full database file (base file) ? It contains both individual IP addresses and subnets. The size of this file is usually in MB.

- The incremental File ? This database has a slightly different format and lesser entries than the full database file. It is available in the form of multiple files throughout the day (in 24 hours). It may contain additions to the base file and/or updates and removals of the existing entries. The incremental database files contain the individual IP addresses (/32 IP addresses).

Login to the Avi CLI and use the `show ipreputationdb <pdb_name> entries filter ip_addr <ip_addr>` command to check if a given IP address is categorized as the bad IP address in the reputation database.

```
[admin:controller]: >show ipreputationdb  System-IPReputation-Webroot-DB entries filter ip_addr 1.2.3.4
```

From the above output, the base file is shown as `wr_ip_ALL_1_2797.txt`. The multiple incremental files are shown as `update_1_2797_1.txt`, `update_1_2797_2.txt`, and so on.

Note: Avi Vantage supports other IP Reputation database service providers in addition to WebRoot.

IP Reputation Sync Interval

The IP Reputation sync interval is the frequency at which Avi Controller polls or sync for the IP Reputation database. The sync interval is modified or configured using Avi CLI and Avi UI.

The default value for the sync interval is 60 minutes. The value of sync interval can be configured any value between 2-60 minutes.

Viewing Events for Debugging IP Reputation

You can view events for debugging IP reputation issues as follows:

Additional Reading

- IP Reputation