HP BAC Anywhere

Pre-requisites to connect on-premise BAC to HP SaaS Cloud

Introduction

HP BAC Anywhere enables the ability to easily extend BAC end-user monitoring coverage to the HP SaaS cloud in an on-demand, subscription-based model. In order to ensure successful connection of your installation of BAC to the cloud, please ensure that the pre-requisites, listed below, are completed.
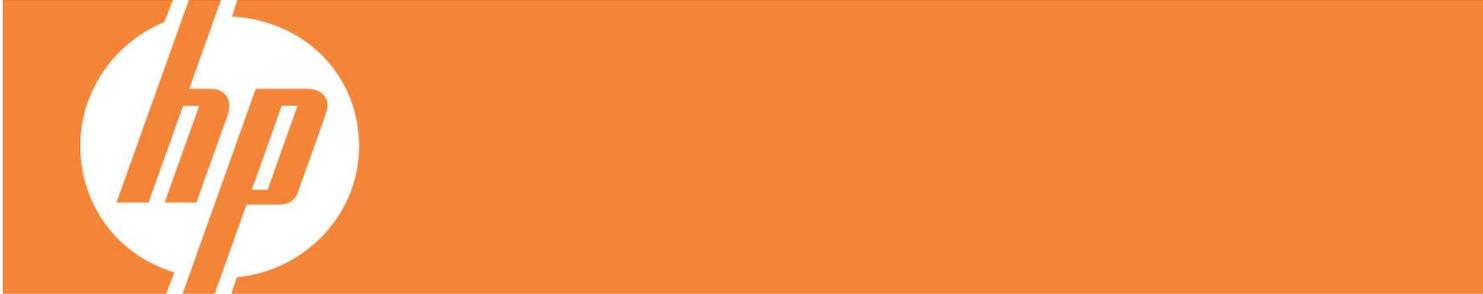
Pre-requisites to successful communication between on-premise BAC and the HP SaaS Cloud

In order to ensure that the on-premise instance of BAC is able to communicate successfully with the HP SaaS global Points of Presence (POPs), please ensure that the you environment is ready and the pre-requisites are completed.

Accepting traffic from Public Points of Presence

The application scripts that simulate end-use experience runs against your networks every periodically. A pattern of periodic network connections are sometimes seen as a "network attack". Therefore, in order to ensure that this traffic is not blocked by your firewall, the IPs to these POPs must be marked as trusted in your firewalls so that the data traffic is not blocked. Your firewall team must open incoming traffic to the POPs. The IPs with masks is defined and is accessible in "Customer BPM Instances" section upon logging into BAC Anywhere.

Secure Connection

HP SaaS recommends that connection between the BAC Server and Business Process Monitor (BPM) client is secure. In order to secure the communication, the BAC server will need to be installed using HTTPS.

If the BAC installation is currently unsecure, a certificate may be purchased from an authorized vendor (like VeriSign*) and installed on the BAC server, per the BAC hardening documentation available on your BAC help files.

If a custom certificate needs to be applied, there will be a need to install the authority certificate on the POP. Please contact HP SaaS support with the details on the client certificate. In such a case, HP SaaS requires 2 weeks to process this request. If further testing of the client certificate be necessary, HP SaaS may request additional time. For this specific reason, HP SaaS recommends the purchase of a SSL certificate from a trusted authorized vendor.

In the case that you have the need to install a proxy server to facilitate the communication between the BAC and the HP SaaS BPMs, the BPM technology provides the flexibility to communicate to BAC through a proxy. In this case, please have the necessary details of the proxy server to configure your BAC to connect to the HP SaaS cloud though the proxy.

* HP SaaS is pre-authorized with the VeriSign certificate