

Horizon Blast Extreme UDP with BEAT Support Functionality in BIG-IP Access Manager 14.0!



Matt Mabis, 2018-22-08

Hey All,

Just wanted to provide an update on new features that were added to BIG-IP Access Manager (Formerly APM) 14.0 for VMware Horizon.

Listed below are the new features that were added into Access Manager for VMware Workspace ONE and VMware Horizon.

- APM supports Blast Extreme protocol over TCP and UDP and also supports the Blast Extreme Adaptive Transport (BEAT) for Desktops and Applications.
- APM supports access to VMware Horizon desktops and applications using VMware Workspace ONE as an IDP for more information on this check out the integration guide at <https://f5.com/Portals/1/PDF/Partners/apm-proxy-with-workspace-one-integration-guide.pdf>

What is the VMware Horizon Blast Extreme TCP/UDP with BEAT Feature?

Since the release of Blast Extreme in Horizon 7, F5 has supported the TCP functionality of the Blast code allowing for the VMware Horizon native client and HTML5 client's to connect to desktops and apps. BIG-IP (14.0) now supports the UDP and BEAT functionality of the Blast Extreme code.

What is BEAT?

BEAT or Blast Extreme Adaptive Transport allows the switching between TCP and UDP of the Blast Extreme Transport based on the connected clients conditions. For example, when a client is connected over a mobile network sometimes the connectivity is unstable (packet loss and/or high latency), with a typical TCP connection packet loss will retransmit the packet over and over again creating lag from a user's desktop or app perspective in Horizon. BEAT was designed to adapt to these types of connections and will detect those packets being lost and adjust the protocol from the connected client from TCP to UDP to allow the dropped packets to be lost and continue moving forward allowing the user to have a more seamless desktop experience. BEAT also has the ability to switch from UDP to TCP depending on the clients connectivity.

Is there an iAPP to Enable Blast UDP?

Currently there is not an iAPP for this functionality and the existing iAPP will only create the TCP functionality for the Blast Extreme Protocol. F5 intends to release a build soon to resolve this issue, this article is being posted to help customers manually create the Virtual Server to allow for the Blast Extreme Functionality prior to the iAPP fix.

Here is the information needed to implement the Blast UDP functionality which will enable BEAT.

NOTE: This will need to be removed when the iAPP is upgraded later to allow for the feature/function

Create a VDI Profile

1. Creating the VDI Profile for Blast Extreme
 2. Navigate to Access --> Connectivity/VPN --> VDI/RDP --> VDI Profiles.
 3. Create a new profile
- Name it whatever you want

Name is whatever you want

- Change Parent Profile to “/Common/vdi”
- In VMware View Settings change from PCoIP to Blast Extreme

The image displays two screenshots of the 'Create New VDI Profile' dialog box. The top screenshot shows the 'General Information' tab selected in the left-hand menu. The main area contains three fields: 'Profile Name*' with the text 'VDI-Blast_UDP', 'Parent Profile*' with a dropdown menu showing '/Common/vdi', and 'Description :'. At the bottom right are 'OK' and 'Cancel' buttons. The bottom screenshot shows the 'VMware View Settings' tab selected. The main area contains a 'Transport Protocol :' dropdown menu with 'Blast Extreme' selected. At the bottom right are 'OK' and 'Cancel' buttons.

Create a Virtual IP for the Blast Extreme UDP Port

- Provide a Unique Name
- Match the Destination Address with existing Horizon APM Deployment
- Service Port: 8443
- Source Address Translation: Automap
- VDI Profile: Select previously created VDI Profile
- Click Finished to Create the VIP

General Properties

Name	VMC-Horizon-APM_blast_udp
Description	
Type	Standard
Source Address	
Destination Address/Mask	172.16.1.15
Service Port	8443 Other:
Notify Status to Virtual Address	<input checked="" type="checkbox"/>
State	Enabled

Configuration: Basic

Protocol	UDP				
Protocol Profile (Client)	udp				
Protocol Profile (Server)	(Use Client Profile)				
SSL Profile (Client)	<table border="1"><thead><tr><th>Selected</th><th>Available</th></tr></thead><tbody><tr><td></td><td>/Common BD-Wildcard-SSL clientssl clientssl-insecure-compatible clientssl-secure</td></tr></tbody></table>	Selected	Available		/Common BD-Wildcard-SSL clientssl clientssl-insecure-compatible clientssl-secure
Selected	Available				
	/Common BD-Wildcard-SSL clientssl clientssl-insecure-compatible clientssl-secure				
SSL Profile (Server)	<table border="1"><thead><tr><th>Selected</th><th>Available</th></tr></thead><tbody><tr><td></td><td>/Common apm-default-serverssl crypto-client-default-serverssl pcoip-default-serverssl serverssl</td></tr></tbody></table>	Selected	Available		/Common apm-default-serverssl crypto-client-default-serverssl pcoip-default-serverssl serverssl
Selected	Available				
	/Common apm-default-serverssl crypto-client-default-serverssl pcoip-default-serverssl serverssl				
SMTSPS Profile	None				
POP3 Profile	None				
Client LDAP Profile	None				
Server LDAP Profile	None				
Service Profile	None				
SMTP Profile	None				
Netflow Profile	None				
VLAN and Tunnel Traffic	All VLANs and Tunnels				
Source Address Translation	Auto Map				

Content Rewrite

HTML Profile:

Access Policy

Connectivity Profile:

Per-Request Policy:

VDI Profile:

Application Tunnels (Java & Per-App VPN): Enabled

ADFS Proxy: Enabled

PingAccess Profile:

Acceleration

Rate Class:

Resources

iRules: Enabled: Available:

Policies: Enabled: Available:

Default Pool:

Default Persistence Profile:

Fallback Persistence Profile:

Local Traffic » Virtual Servers : Virtual Server List

Virtual Server List | Virtual Address List | Statistics

VMC-Horizon-APM Search Reset Search Create...

✓	▼	Status	▲	Name	Description	Application	Destination	Service Port	Type	Resources	Partition / Path
<input type="checkbox"/>				VMC-Horizon-APM_apm_redirect		VMC-Horizon-APM	172.16.1.15	80 (HTTP)	Standard	Edit...	Common/VMC-Horizon-APM.app
<input checked="" type="checkbox"/>				VMC-Horizon-APM_blast_udp		VMC-Horizon-APM	172.16.1.15	8443	Standard	Edit...	Common
<input type="checkbox"/>				VMC-Horizon-APM_internal_https		VMC-Horizon-APM	10.109.1.15	443 (HTTPS)	Standard	Edit...	Common/VMC-Horizon-APM.app
<input type="checkbox"/>				VMC-Horizon-APM_internal_redirect		VMC-Horizon-APM	10.109.1.15	80 (HTTP)	Standard	Edit...	Common/VMC-Horizon-APM.app
<input type="checkbox"/>				VMC-Horizon-APM_pcoip_udp		VMC-Horizon-APM	172.16.1.15	4172	Standard	Edit...	Common/VMC-Horizon-APM.app
<input type="checkbox"/>				VMC-Horizon-APM_proxy_https		VMC-Horizon-APM	172.16.1.15	443 (HTTPS)	Standard	Edit...	Common/VMC-Horizon-APM.app

Enable Disable Delete...

Validation/Testing

Once completed you can test the connection, I recommend using the VMware Horizon Performance Tracker as you can see the BEAT protocol in action changing from TCP to UDP.

VMware Horizon Performance Tracker

At a Glance Session Properties

Machine Name 2K16-RDSH-001
Protocol Blast

Network

Estimated Bandwidth 2.8 Mbps Round Trip 64 ms

Transport

Client to Remote Session UDP Remote Session to Client UDP

Connection Server TCP

Encoder

Encoder Name h264 4:2:0 Bandwidth Used 417 Kbps

Frames/Sec 1 Audio On Yes

Audio Started No

CPU

Encoder CPU 0.31 % System CPU 6.61 %

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com