What's New in the Barracuda Load Balancer ADC

https://campus.barracuda.com/doc/41109454/

What's New in Version 6.5

- **Client Certificate**: Client Certificate can be sent in base64 encoded format to the backend server by configuring X509_HDR_FTR_WHOLE macro.
- **GSLB**: GSLB now supports "@" and "*" as hosts for A, CNAME, MX, TXT, NS record types.

For detailed information on the fixes and enhancements that are included in Barracuda Load Balancer ADC version 6.5, see Release Notes Version 6.5.

What's New in Version 6.4

- **SSL**: Barracuda Load Balancer ADC now supports TLSv1.3 protocol.
- **TCP/UDP**: You can now configure service port ranges for TCP/UDP proxy services..
- **Load Balancing**: Barracuda Load Balancer ADC now supports load balancing Citrix Storefront and Xen App/Desktop.

For detailed information on the fixes and enhancements that are included in Barracuda Load Balancer ADC version 6.4, see Release Notes Version 6.4.

What's New in Version 6.3

Monitoring MYSQL Databases: Support has been added for a new testing method to monitor MYSQL servers.

RSA Secure ID Authentication Service: You can now configure an RSA Secure ID Authentication Service from the **ACCESS CONTROL > Authentication Services > RADIUS** page.

For detailed information on the fixes and enhancements that are included in Barracuda Load Balancer ADC version 6.3, see:

- Release Notes Version 6.3.0.005
- Release Notes Version 6.3.0.004

What's New in Version 6.2

Custom Administrative Roles: You can now configure custom administrative roles.

GSLB Region-Based Failover: GSLB has been enhanced to enable the configuration of region-based failover policies.

SSL Protocol Configuration: You can now specify which SSL protocols should be supported from the Load Balancer ADC's web interface.

For detailed information on the fixes and enhancements that are included in Barracuda Load Balancer ADC version 6.2, see:

- Release Notes Version 6.2.0.005

What's New in Version 6.1

HTTP/2 Protocol over HTTPS: Support has been added for the HTTP/2 protocol over HTTPS.

Microsoft Azure: The Barracuda Load Balancer ADC is now available on Microsoft Azure.

High Availability: The Barracuda Load Balancer ADC on AWS now supports clustering across two availability zones for increased resilience and high availability.

Auto Scaling Groups: Support has been added for configuring auto scaling groups as back-end servers in AWS.

For detailed information on the fixes and enhancements that are included in Barracuda Load Balancer ADC version 6.1, see:

- Release Notes Version 6.1.0.007
- Release Notes Version 6.1.0.006
- Release Notes Version 6.1.0.005
- Release Notes Version 6.1.0.004
- Release Notes Version 6.1.0.003

What's New in Version 6.0

Barracuda Load Balancer ADC models 641 and 642: The latest versions of Barracuda Load Balancer ADC models 641 and 642 leverage specialized hardware to accelerate SSL transactions. These models now have dual power supplies.

Connection Logs: You can now use connection logs to display information about the connections made to the configured services and to the associated servers.

Reporting: A new reporting module has been introduced to the Barracuda Load Balancer ADC with more than 25 reports and built in drill down functions.

Source IP Persistence: Source IP Persistence support has been added at the Service Group level.

Static Source IP Addresses: You can now configure a static source IP address to connect to the real servers.

RBAs: Role Based Administrators (RBAs) are now supported.

Augmented SSL Capabilities:

- Subject Alternative Names (SAN) certificate creation
- SSL Session Resumption
- Strict Transport Security (HSTS)
- SSL Session ID Persistence

For detailed information on the fixes and enhancements that are included in Barracuda Load Balancer ADC version 6.0, see:

- [Release Notes Version 6.0.1.006](#)
- [Release Notes Version 6.0.1.005](#)
- [Release Notes Version 6.0.0.008](#)
- [Release Notes Version 6.0.0.005](#)
- [Release Notes Version 6.0.0.004](#)

What's New in Version 5.4

Barracuda Web Security Gateway service: Enables you to load balance traffic across multiple Barracuda Web Security Gateways (previously Barracuda Web Filter).

VMware VDI over HTTPS and PCoIP: VMware Virtual Desktop Infrastructure (VDI) over HTTPS and

Personal Computer over Internet Protocol (PCoIP) is now supported.

For detailed information on the fixes and enhancements that are included in Barracuda Load Balancer ADC version 5.4, see:

- Release Notes Version 5.4.0.004
- Release Notes Version 5.4.0.003

What's New in Version 5.3

SSL Hardware Support: SSL hardware support is now available.

For detailed information on the fixes and enhancements that are included in Barracuda Load Balancer ADC version 5.3, see:

- Release Notes Version 5.3.0.003
- Release Notes Version 5.3.0.002

What's New in Version 5.2

SSL Enhancements: Perfect Forward Secrecy (PFS) with ECDSA and RSA certificates and associated ciphers are now supported. The key exchange mechanism supported is Elliptic Curve DHE. These SSL enhancements are increasingly relevant in a post-Snowden world. With PFS, communications intercepted today can never be decrypted, even far into the future, due to the ephemeral nature of the PFS scheme. You can also customize backed SSL, including SNI extensions in the TLS header if the server requires this to be enabled. Supports Certificate Revocation List (CRL) and OCSP validation for client certificates. And supports Intel QuickAssist Technology for SSL acceleration in the Barracuda Load Balancer ADC 840 and above.

Traffic Management Enhancement: The Redirect Rule feature is now supported in the Barracuda Load Balancer ADC 340 and 440.

Load Balancer Migration Enhancement: You can now configure the WAN IP address, network mask, and gateway when restoring the Barracuda Load Balancer 4.x backup file to the Barracuda Load Balancer ADC

For detailed information on the fixes and enhancements that are included in Barracuda Load Balancer ADC version 5.2, see:

Barracuda Load Balancer ADC

- [Release Notes Version 5.2.0.004](#)

What's New in Version 5.1

Authentication and Authorization: Barracuda Load Balancer ADC models 540 and above can be integrated with an external authentication server for client authentication. LDAP, RADIUS and Kerberos authentication protocols are supported. You can create authorization policies that control access by authenticated users to web applications.

Application Security: The Application Security subscription, which adds Layer 7 security to your existing HTTP-, HTTPS-, FTP- or FTPS-based applications, is being made available at no charge to all ADC customers on models 540 and above. Configure security policies using the pages under the **SECURITY** tab.

Support for Barracuda Load Balancer Configuration: You can restore backup files from a Barracuda Load Balancer to a new ADC system.

Networking : Policy-based routing to route packets on a specific interface. You can add policy-based routing rules on the **NETWORK > Routes** page.

User Interface

- The **BASIC > Services** page makes it easier to add, edit, and view services and servers. You can view and update every option when you add a service or a server. If you have similar services, you can use the settings of one service as a starting point when creating a new service. And, as before, you can view the status of all services and real servers at a glance.
- The **BASIC > Status** and **SECURITY > Security Policies** pages also have a new layout.
- The web interface has a new color scheme and improved look and feel.
- An Instant SSL service (that redirects an HTTP connection to an HTTPS service) appears as only one service in the user interface. An Instant SSL service includes both the service port and the redirect port.

For detailed information on the fixes and enhancements that are included in Barracuda Load Balancer ADC version 5.1, see:

- [Release Notes Version 5.1.1.004](#)
- [Release Notes Version 5.1.1.003](#)
- [Release Notes Version 5.1.0.x](#)