Load balancing MS-Active Directory and Kerberos

Jeff Browning, 2008-12-09

You know what? You never know what you might find in the DevCentral Forums. Some pretty cool stuff happens in the Solutions Forums - a place to focus on doing interesting things with F5 gear from an application perspective (i.e. Microsoft app, Oracle App, etc.).

Here's an interesting one I found recently: load balancing resources protected by MS-AD-Kerberos. Not always two technologies you expect to see together... However, thanks to user "ravi.rajan", there's the solution. The trick is that you don't add the BIG-IP to the AD (you can't). Instead, you create a Microsoft Service Principal Name (SPN) for "the HTTP services mapping to a particular domain user ids." For more, go here.

For details about SPNs if you're not familiar with them, you can learn more from Microsoft TechNet (a team I worked on many, many years ago, BTW) or at MSDN if that's more your speed.

According to "ravi.rajan", it's not just the IIS folks that get to play:

> ❝We have kerberos single sign on working for IIS, weblogic, SAP enterprise portal without any issues.❞

After talking about this with Colin, he made a good point: once you have this backend wired (and simply doing LB to distinct virtuals/URLs for the various services for IIS, webogic, etc.), why not bring the forms out to the front end and consolidate the process. Theoretically, you could use LTM's form-based auth on the front end. LTM can serve up a standard form and then pass auth through the various services on the backend. Here's a nice little sample (Client Auth Using HTML Forms) in the CodeShare to get you started.

Share this post :▭▭▭▭▭