JANUARY 16, 2014

# The DDI Gatekeeper

by Tim Krzywonos, Manager, Technical Account Management, BlueCat

We've all run into this person before. I'm talking about the "BIND guy" a.k.a the only guy in the entire enterprise who truly knows why DNS or DHCP are setup as they are. You know, the one who answers with, "don't worry, I've got this," when asked a complicated question. The gatekeeper is the type of employee who has their own secret tools to track, troubleshoot and diagnose their DDI environment. And like it or not, the gatekeeper is often viewed as vital to the operation of an enterprise.

Typically, the gatekeeper is the one who implemented the architecture, or was the lucky individual who didn't want ownership of DDI but now holds onto it tighter than a baby does their bottle.

Here's the problem: gatekeepers are a detriment to the modern enterprise.

What sort of challenges do they pose? Let's take a look.

- 1. A single point of failure. If the gatekeeper becomes unavailable (sickness, extended leave, etc.), then core projects will get held up. This costs the business money.

- 2. They're a risk to your business. Gatekeepers will have all the tribal knowledge and they'll know why quirky and intricate configurations were made. They may have planted time bombs in various systems. Remember: we're dealing with core infrastructure here, mistakes can have corporate-wide impact.

- 3. They can be a PITA, or they view themselves as "the ultimate" and employees may not want to work with them unless required. Here's an example: I need some architecture changes done and rather than ask the expert on the best way about doing so, I'm going to try and implement it in another way just so I don't have to talk with the _____ fill in the blank.

We know who the gatekeeper is and the "challenges" they can pose to a company. So, how do you overcome it?

- 1. Simplify. We all know DNS, DHCP, IPAM, automation, etc. weaves a complicated web - especially when the enterprise does numerous mergers and acquisitions, has different factions (i.e. standard IT vs. IT engineering vs. faculty), etc. A standard system with a simple, fluid and

standard UI will ensure common configurations and provide an easy way to incorporate new configurations and systems.

- 2. Allow only common configurations. Use templates. Use approval processes. Automate!

- 3. Who doesn't love documentation? We all look forward to going to work and doing nothing but documentation all day long. That has a sarcastic tone to it, in case you can't tell. Documentation needs to be done, and it needs to be thorough and complete.

- 4. Auditing, monitoring and reporting. No more secrets. When something breaks or isn't allowed on the network, alarms should go off like the building was on fire.

- 5. **SIMPLIFY!** I've mentioned it twice because I can't stress this enough. Specifically, having a non-disparate system. Does the following sound familiar? Where's example.com configured? Oh, it's on the BIND server in Tokyo. Where's company.net configured? Oh, a Windows box in New York. Admins spend more time searching for where things are located than actually doing the required work.

  In short, let's put the above list into one adjective-laced sentence: to rid your enterprise of the gatekeeper, you need a DDI solution that provides simplicity, centralization, security, traceability, scalability and intelligence. With that, your ferocious gatekeeper will be manageable.