Reason #2 That You Need File Virtualization

Don MacVittie, 2009-12-03

If you're just joining us, the first article in this series is here.

While desktop management is a volume issue – touch enough desktops and something is likely to break – Reason #2 is more about complexity. Our data centers are like the cloverleaf on a busy freeway intersection – stuff going every which direction, and no one is quite certain (though some claim to be) what causes all those collisions and slowdowns.

Simplified – and possibly more effective - Security

Yes indeed, I did say that. And I mean it. I figure that once it's explained, even my Security friends will have to agree.

NAS access control has never been a very good thing. Most organizations have worked it out to be minimally successful, but there are still gaping holes that an attacker, once through the outer defenses, has a fertile field to sow in. Sadly, "attacker" includes rogue employee, who, like a fifth columnist is already inside the outer defenses.

Even if you have a centralized NAS system from the likes of NetApp or HP, you still have the issue of all those other servers in your organization that have shares on them. Even if you are using centralized access control through AD or LDAP, you still have the issue that 5 million shares need to have rights set on them on 2 million boxes. Okay, I way exaggerated the numbers, but you get the point – you've seen it, and if you're unlucky, you've lived it.

Most File/NAS Virtualization devices offer you the ability to say "only allow changes through our device". This sounds like a play to make them integral to the infrastructure. The truth is that sometimes it is necessary if you are going to use a device that operates off of metadata to guarantee that it has a chance to update the metadata whenever something changes.

It turns out that with just a bit of thought about implementation you can turn this into a huge plus.

You have three servers with shares on them in your marketing department. Let's call them *campaigns*, *pressServer, and marketingResources*. **These three machines have a total of five shares. They're all closed down to everyone except the marketing group. So you've got the group of users, five shares, and two machines to maintain for access rights purposes. Should more shares be required (and they inevitably will if the group is active), you have to set up the access rights on those also. Should a server crash, you have to recreate access rights when the replacement is put in.**

Enter the File Virtualization appliance and its lock-down capability. I haven't looked in this space for a while, but last I looked they all allowed lock-down by IP (so only the Virtualization appliance's IP can access shares), by username (so only the account the appliance/device runs as can access the shares), or both. ARX allows for both. Since the Virtualization appliance is a proxy for all users that run through it, this is not a problem. So you lock down all the CIFS and NFS shares that will be behind the File Virtualization device, and then you import everything into the directory tree (actually usually done in the opposite order, but this order was better for our example). This is where the secret sauce comes in. You put all five shares on the marketing servers under a folder called *Marketing*. **Then you set rights on the** *Marketing* **folder to restrict to your group. The key here is** *you do not have to restrict anything else*. **Now every share/folder/whatever that is in the tree underneath the** *Marketing* **folder will automatically get the level of access and user rights set for the Marketing folder. And if you replace one of these servers, just adding it back in under Marketing automatically sets rights.**

Most of these products will go out to AD or LDAP to retrieve access rights and group membership info, so it's not like you're replacing anything other than where groups are assigned rights to a share. In the normal world you have to do group-server-share combinations, in a Virtualized environment you can ignore the server and just do group-share. By moving that combination up the directory tree, you remove an entire element of security management complexity. You also have one less step when creating a new share – no matter what platform the share is on, it inherits rights from it's parent folder in the virtual directory.

Of course some organizations are what I call "Exception a Minute" organizations, where access rights to things under the Marketing folder might have a list a mile long of IT, Sales, and Janitorial staff that *simply must have access.* **I'm afraid File/NAS Virtualization won't solve that problem for you, only policy and process at the corporate level can do that.**

Since Justin asked about tiered storage and it is a *big win***, we'll hit on that one next week. Until then, enjoy!**

Don.

Share this post :

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

F5 Networks, Inc.	F5 Networks	F5 Networks Ltd.	F5 Networks
Corporate Headquarters	Asia-Pacific	Europe/Middle-East/Africa	Japan K.K.
info@f5.com	apacinfo@f5.com	emeainfo@f5.com	f5j-info@f5.com