







This review was carried out by ZDNet in the first week of December 2008. It is reproduced below with the permission of ZDNet, and can be found on the ZDNet site at:

<http://reviews.zdnet.co.uk/hardware/networking/0,1000000696,39574100,00.htm>

8.0 Editors' Rating **EXCELLENT**

Service & support		8.0
Features		7.0
Setup & ease of use		9.0
Performance		8.0



Roger Howorth ZDNet.co.uk

Published: 08 Dec 2008

Running an IT infrastructure without a proper disaster recovery (DR) plan is reckless, given the vulnerability of IT systems and our dependence upon them. The problem is that DR plans require a mixture of services such as offsite storage, replication and networking that are tricky and expensive to put together. This is why many businesses — especially small and medium-sized ones — will be interested in a new appliance and service offering from [Plan B Disaster Recovery](#).

Plan B, a UK company based in Berkshire, uses an on-site appliance to make daily snapshot backups of your servers, which are sent to the company's datacentres via secure internet links. These snapshots are used to create virtualised replicas of your servers at the Plan B datacentre, and these virtual servers (Plan B calls them 'rescue images') are tested each day to make sure they boot properly without errors. Plan B also creates IPsec VPN links between your office and the Plan B datacentre, so the replacement servers can quickly and easily be reconnected to the company LAN. It can also run extra DNS servers to reroute traffic to the replicas in the event of the main systems going offline.

Plan B says that it can replace a client's servers within 30 minutes of the main systems going offline. In a full-on disaster scenario where all of a client's normal IT systems become unavailable, users can connect to the Plan B datacentre from any PC or notebook using a web browser and SSL-based VPNs. Once a suitable replacement office is available, it would be connected to the rescue images using the IPsec VPN. A three-year contract for 50GB of data will cost you £1,135 (ex. VAT) in setup fees plus a service charge of £200 a month.



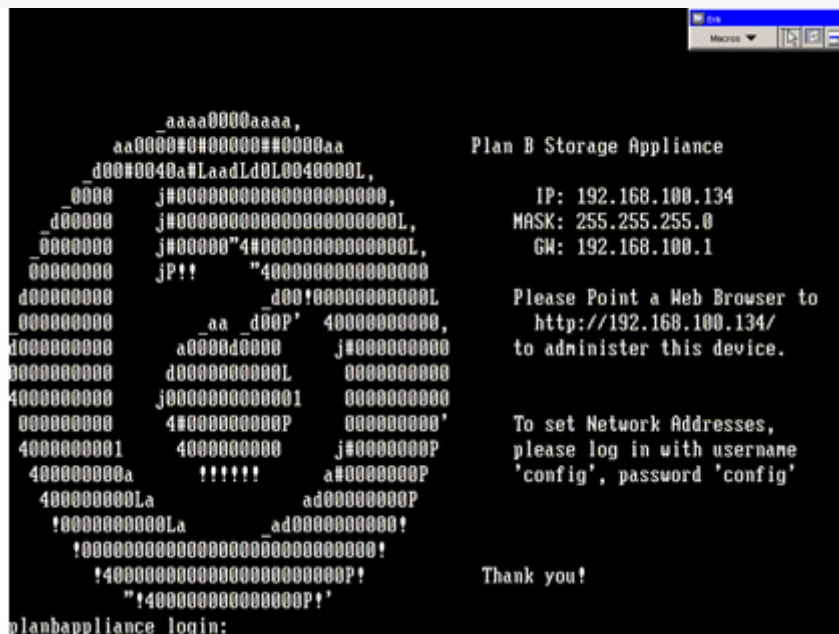
Plan B's appliance plugs into your network and takes daily snapshots of your servers, which are then sent to the company's datacentre where virtualised 'rescue images' are kept.

We tested the Plan B DR service in ZDNet UK's Labs by configuring the appliance to protect one of our servers running Windows Server 2003 Small Business Edition. Currently the appliance is compatible with all forms of Windows Server from 2003 onwards; support for a few Linux distributions is expected to be added soon.

One of big advantages of Plan B's offering is its simplicity of setup and management. In our tests, the first step was to fill in a simple email questionnaire that briefly described the servers we wanted to protect. This helps Plan B get a handle on things like the Windows Active Directory structure, network topology and the services running on the servers. It also provides an opportunity to exclude certain directories from the snapshot backups. For example, we excluded several local disk drives that store backup data because we didn't want to slow down the transfer of snapshots unnecessarily by moving this data around.

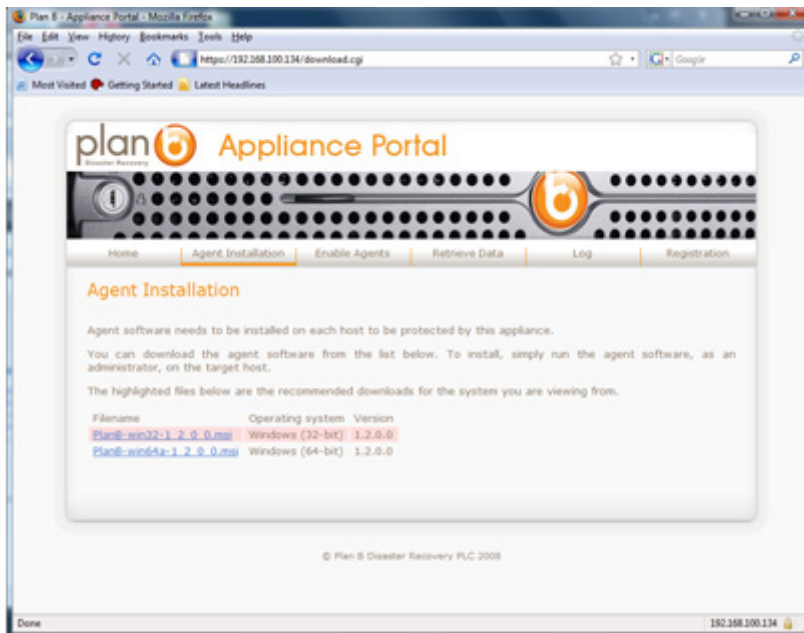
We also were able to specify how our internet bandwidth would be used to send data to Plan B. We took the default options, which were to limit bandwidth to 10KB/s during working hours, and to allow all our bandwidth to be used after 11pm. It took us about ten minutes to complete the questionnaire.

Next we installed the Plan B appliance, which merely involved fitting the 1U server in our datacentre rack and connecting it to mains electricity and the LAN. The initial configuration requires a keyboard and monitor to be connected to the appliance, but once the setup is complete these can be removed.



The Plan B appliance's text-based welcome screen.

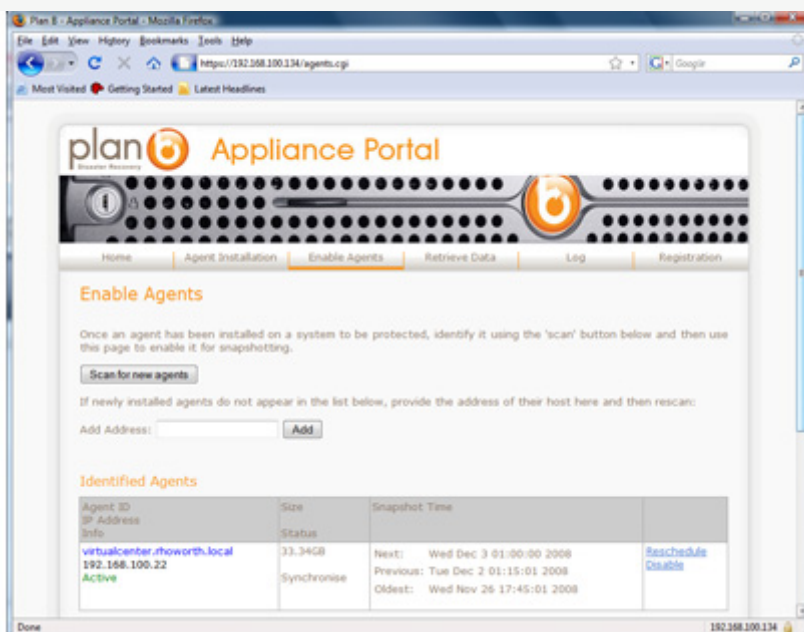
Once the appliance was switched on, we were greeted by a text-based welcome screen asking us to log into the initial configuration menu. The username and password for this were shown on the screen. Once logged in, some IP settings are required, so we told the appliance to retrieve suitable information from our DHCP server. Then we entered our customer ID and appliance ID, both of which had already been sent to us by email. Finally we typed in what Plan B calls the 'bootstrap password', which was imparted during a phone call with the company's engineers. Changes can only be made to the appliance configuration by entering a bootstrap password, and a new one is needed each time a change is made, so system administrators need to contact Plan B and request a new bootstrap password before they can update the appliance configuration.



Downloading a Win32 agent onto the target server from the Plan B appliance.

The next stage is to install an agent onto the server you want to protect so that the appliance can make snapshot backups. The agents are downloaded and updated via the appliance, so the next step in our installation process was to connect to the appliance's web-based management console from the target server. Again, Plan B had already supplied us with suitable login credentials. Once logged in, we selected the agent installation menu option and downloaded the Win32 agent. Installation onto our server was very quick, and when it was completed we used the Windows Services management tool to confirm that the Plan B service had been properly started. No reboot was required.

The agent makes backups of the servers using Microsoft Volume Shadow Copy Service, so it's compatible with a wide range of applications and can make snapshot backups with only a momentary freeze of the Windows environment.

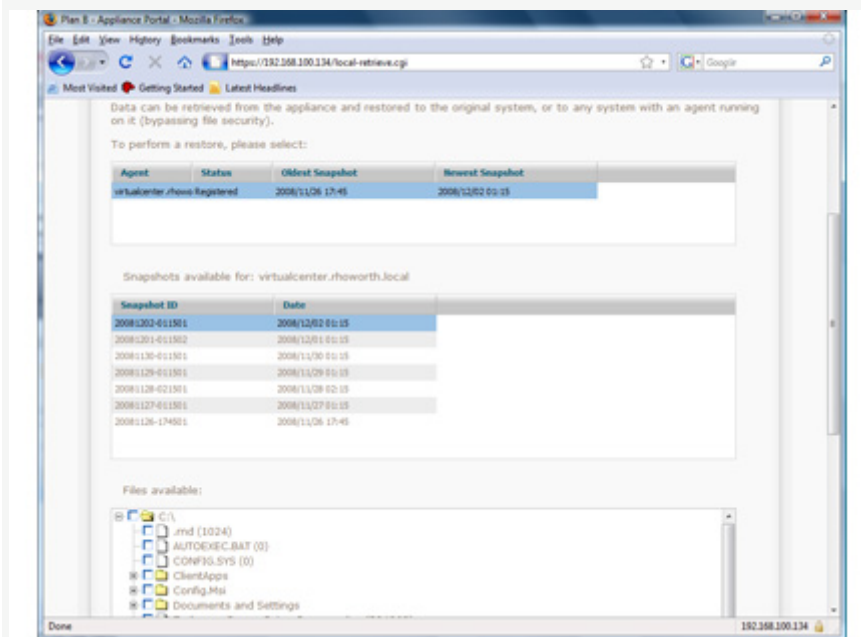


After enabling the agent from the Plan B appliance and ensuring that the target server's virtual counterpart is ready at Plan B's datacentre, snapshots can begin.

Next we used the Enable Agents option in the appliance management portal to scan the network for our newly installed agent. The scan worked like a charm, and once located we could easily enable the agent by clicking on a link. This completed all of the necessary setup at our end. However, before the appliance can begin taking snapshots, the server must be enabled at the Plan B datacentre. The Plan B operators did this as soon as they noticed our setup was active, so the first snapshot was made and transferred to the appliance almost immediately we completed our installation.

The initial snapshot is likely to contain a lot of data — in our case the server's C drive had some 40GB. Understandably this took a few hours to transfer to the appliance, and then quite a lot longer to transfer to the Plan B datacentre. With our internet connection and bandwidth settings the first snapshot was transferred after two overnight sessions. We received a phone call from Plan B to tell us the first transfer had finished, and the engineer confirmed that our rescue image had booted properly.

We tested a disaster recovery scenario by phoning Plan B to ask them to activate our rescue image. They called back about ten minutes later with details of how to connect to the datacentre via a web browser and an SSL VPN connection. We could then connect to our virtual server and its web-based management tools using Microsoft Terminal Services. Although the rescue image had a different IP address to the original server, its applications worked perfectly. We normally manage our Labs server using [LogMeIn](#) remote control software, and this was also available and working on our virtual replica without needing to use the VPN.



Files and directories stored on the Plan B appliance can be restored to your server via the management portal's Retrieve Data option.

Our Plan B appliance had 638GB of storage capacity, and an added bonus is that system administrators can restore individual files and directories from the appliance by logging into the web management portal. We tested this by clicking on the portal's Retrieve Data menu option and selecting a snapshot from a list of those stored on the device. This produced a hierarchy of the files, and from here we could drill down into the directory structure and select the files to be restored. Files could be restored to their original location or to any other server running the Plan B agent.

Conclusion

We were very impressed by Plan B's service, which we found straightforward to set up and configure. Part of the Plan B offering is to ensure that the rescue images are transferred properly every day, and the company will notify customers if this doesn't happen properly. So once up and running we were confident we could leave it to get on with things.

As far as maintenance is concerned, the appliance receives software updates and patches automatically via its connection to the Plan B datacentre, and it distributes updates to the agent software as required — all without rebooting the servers that are being protected.

Besides the monthly service charge and setup fees, there is a disaster invocation fee of £400 to activate each virtual machine, and other charges if you don't get your servers back online within two weeks. Plan B recently had an [ISO 27001](#) Stage 2 audit, and expects to have this certification within a few weeks of this review's publication.