Complete backup solution from a single source

Dr. Götz Güttich

With its backup appliances, Arcserve offers enterprise-class backup solutions for disaster recovery and application availability. The products not only provide powerful backup software that can be controlled via a web interface, but also the hardware required to efficiently perform backups. This includes the necessary storage capacity so that administrators do not have to purchase additional components to implement their backup strategies after purchasing the appliance and installing it in the rack. In the test, the product was able to show what it is capable of.

Backup appliances are particularly suitable for use in decentralized environments, branch offices or smaller companies. However, they can also be used as primary backup in larger networks. The deployment options of Arcserve Appliances include single-site, primary-site, cross-site and central appliance-site scenarios.

The appliances work with Arcserve's Unified Data Protection (UDP) backup software, which was available to us in Version seven at the time of testing and supports technologies such as data compression and deduplication. On the hardware side, the systems are based on reliable hardware from one of the leading server hardware makers with flash-accelerated memory, high computing power, Gigabit Ethernet connections and redundant hardware.

According to the manufacturer, the appliances should be up and running in 15 minutes. Not only are they capable of backing up physical machines running Linux and Windows, they can also back up virtual machines (VMs) from Microsoft and Vmware virtualization environments. In addition, users use the products to back up Office 365 environments, Exchange servers, SQL servers, Oracle installations, Amazon AWS and Microsoft Azure workloads, and – when Arcserve Backup is installed – also Nutanix, as well as OS supported by Arcserve Backup: Solaris, AIX, HP-UX, FreeBSD and IBM System z mainframes. The data backups themselves take place either locally on the appliance or on external storage, as well as in private or public clouds.

The solutions support the cloud services Amazon AWS, Arcserve Cloud (where customers can rent storage space for their backups), Eucalyptus, Microsoft Azure and Rackspace. Cloud storage is particularly suitable for collaboration with the Arcserve Appliance because the associated backup software has its own highly efficient source-based deduplication

technology that reduces the need for bandwidth and cloud storage.

Bare metal restores (BMR), replication and granular restores are also part of the appliance's capabilities. The solutions also support hardware snapshots, high availability, and tape drive collaboration.

If required, additional hard drives can be added to the products to increase storage capacities needed. Up to 504 terabytes of storage are available on one appliance. The central management interface allows up to six petabytes of backup data to be managed in one place.

In practice, the appliance should enable a "set and forget" strategy. For this reason, they are configured using wizards that cover their initial setup configuration.

The Test

For the test, Arcserve provided us with a 9240DR Appliance with two Intel Xeon Silver 4114 2.2G CPUs, 192 GB RAM and a PERC H730P RAID controller. This came in two height units and offered us four Gbit Ethernet interfaces for connections to the networks to be secured and an additional interface for remote access to the server. The storage capacity of our appliance was 72 terabytes binary, but devices of this type can be expanded up to 168 terabytes. The storage was configured as a RAID-6 array and two additional 1.9 terabyte SSDs as caches were included in the scope of services, which were configured as a RAID-1 array.

In the test, we put the system into operation, backed up Linux and Windows systems, secured VMs of Hyper-V hosts and Vmware ESXi hypervisors, and backed up an Office 365 account. In addition, we ran restore operations and outsourced the backup data to external devices.

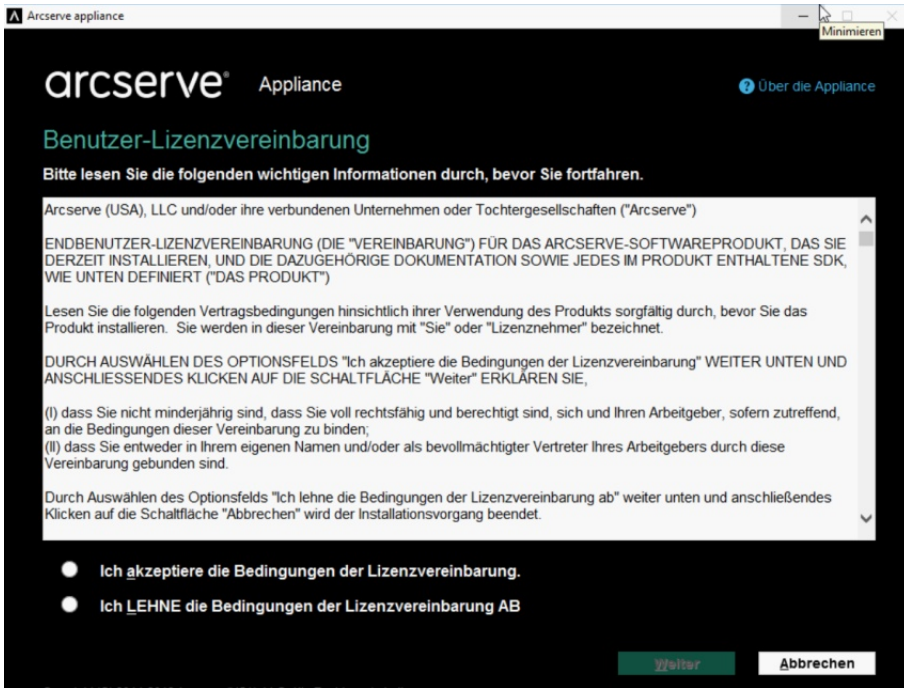
Initial setup

In order to put the solution into operation, we connected the appliance to our LAN via its regular interfaces and via the appliance interface. Then we supplied it with power and booted. The appliance interface received an IP address from our DHCP server, which was shown on a display on the front of the device. We were then able to connect to this IP address via our browser and access the system's console.

Alternatively, since this is standard server hardware, there is also the option of connecting the keyboard, mouse and screen directly to the appliance and performing the initial configuration locally. The operating system used on the appliance is Windows Server 2016. After the first boot process, this system first asked the console for the language settings to be used and asked us to accept the licensing conditions. After that, a restart was due.

After completing the second boot process, we first had to set an administrator password and log on to the system. Then the Arcserve Appliance Wizard started automatically. This first displays license information and then allows administrators to change the host name and join a domain. Another restart is then due.

After this reboot, we configured the local interfaces of the system – also using the wizard – so that they worked with a fixed IP address. Then the appliance was accessible via the URL https://{IP-address of the system}:8015 via browser.



The initial setup of the appliance is done via a wizard on the local console of the operating system

This whole process already shows that the Arcserve Appliance is not – like many other appliance offers – a closed system, but – as the manufacturer says –

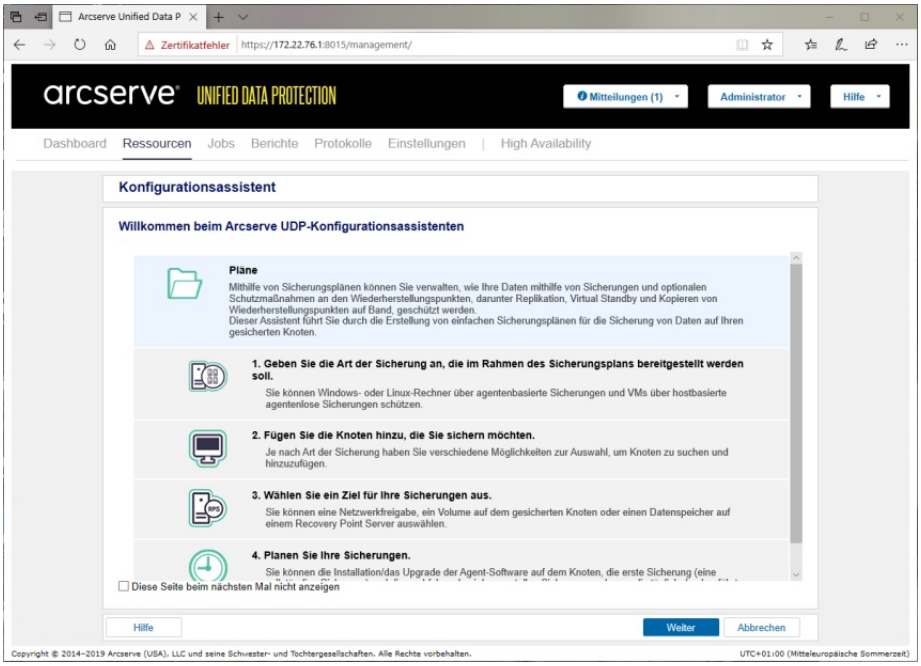
an open appliance, where the users have access to the underlying operating system. This opens up extensive possibilities to adapt the system to their own requirements. For example, customers can install their own antivirus solution on the backup system if required.

Scheduling backups

At the end of the setup phase, the next step was to set up the backup environment using the UDP Plan Configuration Wizard. The wizard wants to know whether the appliance is a standalone instance or whether the product should be managed from a different console. Since we had only one device in the test, we chose the first option.

The wizard then displayed the storage configuration and wanted to know the password that would be used to encrypt the backup data. In the next step we had the possibility to configure e-mail notifications. This can be configured either for successful jobs, for failed jobs or both. The wizard then asks for the remote restore point server. This can be used, for example, if an Arcserve backup server already exists in the network. We overlooked this point in the test, since we were working with a standalone system.

Now it was time to define our first backup plan. We first had to enter a session password to secure access to the session. This way it is possible, among other things, to allow only certain administrators to access certain backup sessions.



The UDP Configuration Wizard helps to create a backup plan

We were then able to select one or more nodes to back up from our network. For Windows devices, this can be done by host name and/or IP address, by selecting the nodes from the Active Directory and by importing them from vCenter/ESXi or Hyper-V installations. In the test, we first selected a physical Windows 10 client (version 1903) from our Active Directory, which the appliance was supposed to completely secure.

The last step in defining the back plan then consisted of creating a schedule. We set up the system so that it first installed the backup agent on the target system at 12:30 on a Tuesday. In the following weeks, this job was used to update the agent if necessary. In addition, we also specified that the daily backup should start at 13:00. The first time the system backs up the computer completely, the next backups are incremental. In this context, users can determine how many recovery points the system has to maintain. If the maximum number of recovery points to be stored is reached, the system automatically merges the last recovery point with the full backup. The administrators do not have to worry about this and it is also not necessary to create new full backups during operation.

Once the plan has been defined, the initial setup is complete and the appliance starts working. Afterwards the system behaved as expected during the test, took the agent out on our client at the specified time and carried out the backup half an hour later. Overall, it took more time to get the appliance up and running than the promised 15 minutes, but this was mainly due to the multiple boot operations that took some time on the server hardware. As far as the actual effective working time is concerned, the manufacturer's statement of 15 minutes should in principle be realistic.

The next backups

The backup plan of our Windows 10 client remained in operation throughout the entire test and reliably created differential backups of the affected system

every day after the first full backup. The next step in the test was to back up a Windows Server running Windows Server 2019.

We added the server as a backup node from our Active Directory to our Arcserve environment and set up a corresponding backup plan. As with the Windows 10 client, the appliance first installed the agent on the computer to be protected and then performed the backup. Backing up Windows computers is obviously not a problem.

Data recovery

At least as important as a successful backup is the recovery of the data. In this context, Arcserve offers to completely restore all data, select individual data and perform the recovery to the original location or to an alternative destination. In the test we decided at this point to restore the complete "Users" directory of the server to an alternative location. As a target, the appliance offered us all local drives on the appliance itself, including shares previously connected via Windows. So the restore process to a network share that was accessible for everyone was no problem.

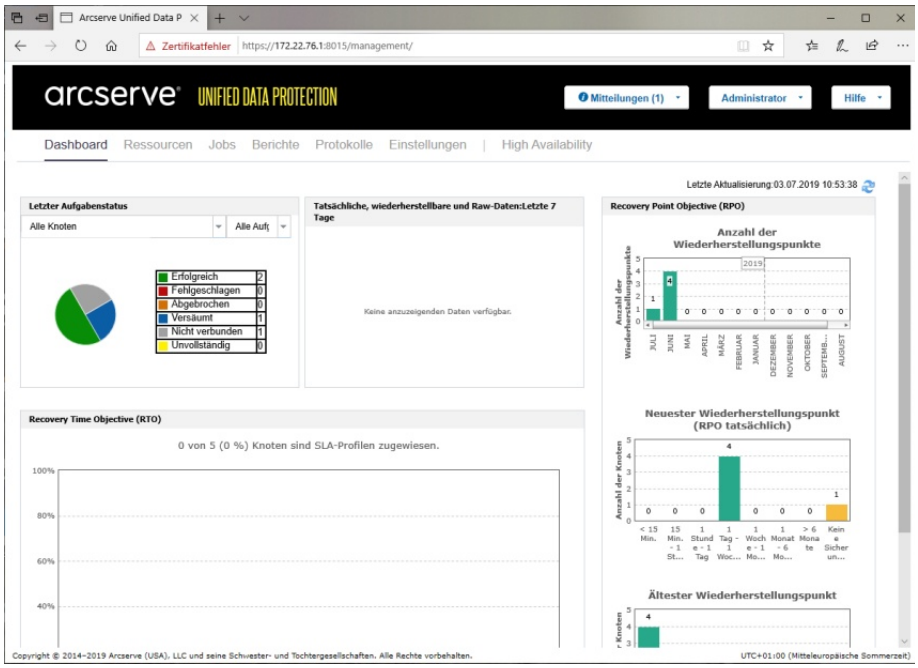
Backup of a Linux system

The backup of a Linux system works similar to Windows systems. When inserting the Linux node, you have to give the appliance the SSH access data next to the computer name or the IP address, then you can back up the data on Linux systems. For this to work, the backup software also needs a so-called Linux backup server. This was set up as a virtual machine under Centos 7 on a Hyper-V basis directly on the appliance, so the users do not have to deal with it separately. Once a Linux backup node has been defined, the data backup then runs exactly the same way as with Windows using plans. In the test, we successfully secured machines under Centos 7 in this way.

Backing up virtual environments

Next, we looked at the backup of virtual machines working in Microsoft Hyper-V and Vmware ESXi environments. First, we had to add our hypervisors, which were running on Windows Server 2019 and Windows Server 2016 for Hyper-V and using ESXi 6.7 Update 2 for Vmware, as nodes to our backup environment with the appropriate credentials. The appliance then connected to the appropriate systems and indicated which VMs were present on them. We could then simply select them and start or schedule the backup. In this context, it is also important to know that the VMs should run under Hyper-V during the backup process, otherwise the system will not be able to access the Volume Shadow Copy Service (VSS) of the affected virtual machine, for example to perform consistent backups of SQL Server installations using snapshots. If this functionality is not important, the backups can also be created from switched off machines. The actual backup process is not affected.

In general, it was no problem to create the backups of the VMs. The restore process also went as expected. Again, it is possible to restore the entire VM or individual files and folders.



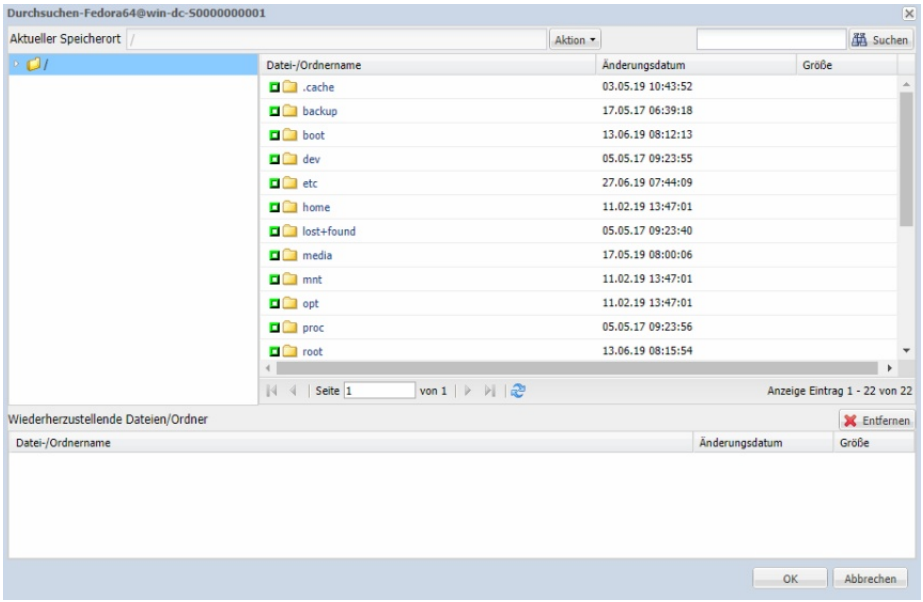
The dashboard provides information about the overall state of the system

In Vmware environments, you should know that the free ESXi license does not allow backups with any Backup solution, so also not with Arcserve. If you use a free Vmware hypervisor, you can still back up the VMs on it like physical computers using agents.

Office 365 backups

Arcserve also offers backups of Office 365 accounts. The system distinguishes between OneDrive, Exchange Server and SharePoint backups. In the test, we backed

up OneDrive from a normal Office 365 business account. But first we had to activate the corresponding functionality. To do this, it is first necessary to use the "Install-Module AzureAD" command to import the corresponding module via Powershell. We also had to change the execution policy (also via Powershell) to



Data recovery from a Linux computer

"Remote Signed": "Set-ExecutionPolicy RemoteSigned".

When that was done, we created a backup plan for an Office 365 OneDrive backup, specified the appliance as the backup proxy, and entered the credentials of our Office 365 subscription. A browser window then opened, allowing us to give the Arcserve UDP application the right to access the Graph API of our Office 365 account. The security node was then available and we were able to integrate it into our backup plan. In operation, the backup then ran as planned.

Outsourcing backup data to external storage media

In real life, it makes no sense to keep backups in one place only. Therefore the Arcserve Appliance allows you to automatically copy the data of created backups to other storage media.

All administrators have to do is go to the backup plan whose data they want to copy and add a new task within the plan configuration on the left. The task type in this case is "Copy recovery points" and allows you to specify a local disk, such as a USB storage device, or a network share or cloud storage as the copy destination.

If Arcserve Backup is installed, also a tape device can be attached. In the test, we used a network share defined by a UNC path for this purpose. There were no problems. The tasks can also be used to perform other actions during operation, such as storing backup data on tape drives.

Dashboard, analyses and reports

A backup solution would be worth little if the administrators remained unclear about their actions. That's why the Arcserve Appliance not only provides a dashboard with up-to-date information about the status of tasks, the number of recovery points and the like, but also powerful analysis and reporting tools. The latter, for example, provide information about the trend in backup sizes so that the responsible employees can see how long the existing backup storage will be sufficient.

There are also graphically illustrated reports that show what the backup status of the nodes in the network looks like and, for example, indicate if backups have been missed or interrupted. Similarly, those responsible are able to view the occupied storage space or access the system logs, among other things.

Conclusion

The backup appliance from Arcserve fully convinced us in the test. The solution is easy to set up and provides a complete backup environment out-of-the-box with all necessary components and a powerful deduplication function. This can be easily managed due to the central management interface and it is also possible to add external assets.

Thus, other Windows servers in the network can be used as additional recovery point servers at any time. In this case the mentioned systems are used as a second backup server. No additional licenses are required. When licensing, Arcserve follows the policy that only one license must be available to create the original backup. Users can then export the backup data from the appliance as often as they want. Due to the large scope of performance and the good usability, we award the product with the rating "IAITested and recommended" to the one that has little to criticize (only the documentation could be clearer).