

Business Continuity with ReadyNAS[®]

What is ReadyNAS®?

ReadyNAS® is a family of network storage solutions for small and medium businesses, workgroups, and remote/home offices. ReadyNAS delivers unified storage through multi-protocol NAS and SAN support in an affordable storage appliance. Firms with less than 500 users rely on it as primary storage for file serving, disk-based backup, and virtual environments, while larger firms use it as secondary storage or in branch offices. Automatic volume expansion, integrated snapshots, replication and an embedded cloud backup option make it a versatile platform for building solutions at price points unreachable by traditional storage vendors. All of the ReadyNAS product family is based upon the common RAIDiator operating system, which offers simple interoperability between all ReadyNAS systems, and ReadyNAS for Business systems are Microsoft Hyper-V and Citrix compatible, and VMware Ready. This paper describes how to create a disaster recovery (DR) environment using the native tools common to all ReadyNAS for Business products.

Snapshot Overview

Snapshots provide organizations with an added level of data protection that has minimal impact on production environments. By setting up periodic snapshots, users can have a complete second copy of their data at a given point in time (PIT), without incurring the expense and delay of making a full copy of the data. Snapshots provide instantaneous clones of data by cataloging all files but only making copies of files if they are altered after the snapshot was taken. In other words, snapshots are a PIT or “on the box” insurance policy.

One common use is the rolling snapshot. For example, creating a snapshot that executes daily at midnight would capture the state of the storage environment at that time. The advantage is having a fall back copy of data that is only hours old from which one could quickly restore in case of corruption, accidental loss, or malicious behavior. If a shorter period of exposure is desired, then snapshots can be taken more frequently. Since snapshots are not application aware, they protect any type of data or file. Hence, snapshots provide an extra data protection assurance in file sharing environments and general-purpose protection of generic unstructured data sources in between scheduled full system backups.

NETGEAR® ReadyNAS systems fully support snapshots to provide organizations with a very efficient and low-cost solution to protect data integrity. The near instantaneous operation and marginal demands on storage resources provide an easy safety net against PIT data loss or corruption. However, snapshots are not designed to protect against hardware or equipment failures; this is where the complimentary protection offered by replication comes into play.

Replication Overview

Replication enables organizations to copy and distribute data and files across multiple storage solutions within the datacenter, branch offices, and/or other locations. Replication can be scheduled or take place on demand. As such, the act of replication provides the basis for periodic backup and DR solutions that protect against hardware or equipment failures, natural disasters, or other external threats. In addition, replicating data can deliver performance improvements by having the data physically closer to the applications that are driven by the data.

NETGEAR ReadyNAS systems use rsync technology for secure block-level replication. However, manageability and ease of use are primary design considerations so a graphical user interface dramatically simplifies replication management in more complex scenarios. Organizations can implement ReadyNAS replication without specialized storage management professionals. All ReadyNAS products are interoperable — any ReadyNAS can replicate to and from any other — and data can be encrypted during the transfer, eliminating the need for a VPN.

Common Disaster Recovery Scenarios

ReadyNAS is an excellent platform for businesses seeking DR solutions in main data centers, branches, and/or home office locations. Customers may recover operation from a physical interruption in service due to a large-scale equipment failure, utility outage, or natural disaster. The focus is on achieving the fastest uptime (Recovery Time Objective) and returning to an acceptable known point (Recovery Point Objective). The combination of periodic snapshots with offsite replication provides a DR solution that protects organizations against unforeseen service interruptions and enables rapid recovery. The following sections highlight five scenarios where ReadyNAS provides a viable DR solution without any additional software or expertise requirements.

Traditional Physical Server Environment

Providing offsite protection for a traditional server environment is easily achieved by adding ReadyNAS to an existing backup solution or new IT environment. This scenario typically involves physical servers running Microsoft Windows or Linux and a combination of existing direct attached and/or networked storage.

Most commonly, using existing 3rd party backup software (such as products from Acronis, Symantec or StorageCraft) the ReadyNAS is configured as a backup to disk target (tape replacement). The ReadyNAS acts as a backup repository for the servers' backups. The number of servers and size of production data generally determines the most appropriate ReadyNAS models to deploy; if needed, additional ReadyNAS devices can be deployed to improve overall performance and provide scalability. With a maximum capacity of 24TB and 10GbE Ethernet for throughput the ReadyNAS platform can provide a backup location for nearly any business customer.

The choice of backup software is a key consideration as the efficiency of the ReadyNAS replication and the storage capacity required will be directly related to the sophistication and capabilities of the backup software. Backup software that includes intelligent backup/storage techniques such as de-duplication, incremental block level backups, and synthetic full backups will greatly assist in disk and bandwidth savings when replicating data.

The replication provided by ReadyNAS is based on rsync technology that allows data to be replicated at the block level; this means only changed blocks of data need to be migrated between two ReadyNAS devices. The more efficient the backup software is when writing new backups the less data will be replicated offsite.

Building a ReadyNAS backup solution is as simple as deploying a primary ReadyNAS as a backup target that is configured to replicate to a secondary offsite ReadyNAS. This replication target might be at a hosted data center, a value added reseller's (VAR) data center or even, in smaller scenarios, a home location.

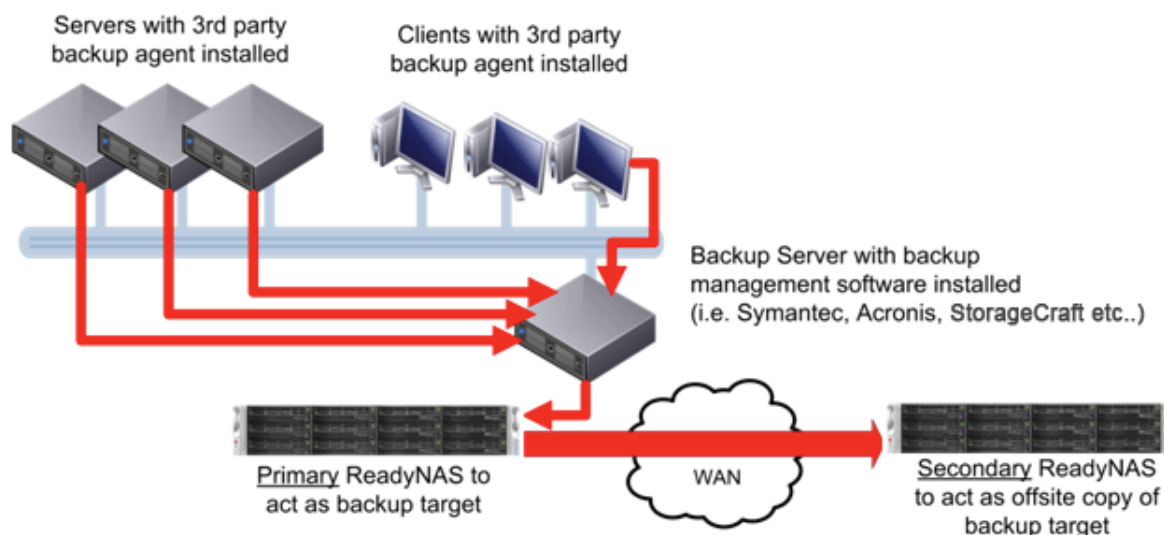


Figure 1. Protecting a physical server environment with ReadyNAS

The ReadyNAS for Business product line meets the primary replication needs of most companies with less than 500 users (see current model specifications for performance and capacity data). As with backup, the choice of 3rd party backup software can significantly impact replication efficiency. Acronis, Symantec, and StorageCraft all provide an efficient backup software solution that work with ReadyNAS storage.

ReadyNAS as Backup Target for Virtual Server Environments

ReadyNAS can be used as a storage solution for the backup of existing virtual server environments. This scenario involves adding ReadyNAS into a virtualized environment where virtual machines (VMs) are executing from storage other than ReadyNAS.

Using either 3rd party backup software such as Veeam, Vizioncore or the built-in backup function of the hypervisor such as VMware VDR (VMware Data Recovery), the ReadyNAS is configured as a backup to disk target for the VMs. As with physical server environments, the ReadyNAS acts as a backup repository for the server(s) but with the added benefit of capturing the complete VM environment including the server configuration, operating system, applications, and associated data files whenever a backup is created.

The choice of backup software is critical as it will need to be well suited for virtual environments especially with respect to de-duplication given the tremendous commonality of data between the contents of VMs based on similar operating systems.

The primary ReadyNAS is configured to store complete backups of VMs and those backups replicate to a secondary offsite ReadyNAS. The VMs can then be restored onto another 3rd party virtual environment or directly onto the secondary ReadyNAS. By powering up VMs directly on a ReadyNAS the restoration process onto the remote server can be skipped since the secondary ReadyNAS can act as both an offsite backup and a VM repository for live VMs. ReadyNAS can be used with Hyper-V and Xen, and is VMware Ready (supporting both iSCSI and NFS protocols).

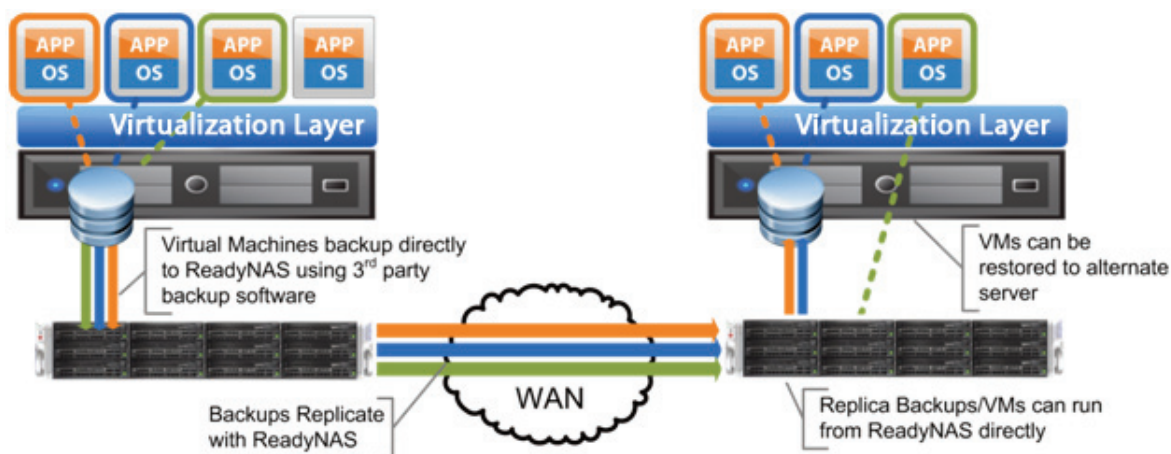


Figure 2. Adding ReadyNAS as a backup target to existing virtual environments

In some cases restoration can be as simple as attaching a hypervisor to the ReadyNAS and starting up the replicated VMs. This method makes it easier to get system state up and going faster after a disaster scenario. DR is predicated upon rapid restoration of service, that is achieving an organization's Recovery Point Objective within its Recovery Time Objective; this is where leveraging the ReadyNAS multiprotocol functionality really assists with recovery.

ReadyNAS as Primary Storage for Virtual Environments

NETGEAR supports using a ReadyNAS array as a virtualization storage platform for running live VMs. Deployment of ReadyNAS with VMware, Hyper-V or Citrix Xen Server is fully supported. Replicating VMs from one ReadyNAS to another, combined with application backup, offers an integrated DR solution for virtual server environments. This scenario would typically be found in a smaller environment where performance levels offered by SATA storage and ReadyNAS hosted VMs meet the production needs of a few workers, test and development environments, or secondary sites.

The primary ReadyNAS is configured to replicate to a secondary offsite ReadyNAS. Using snapshots will capture complete VM environments including the server, applications, and associated data files. The VMs can be immediately powered up on the secondary ReadyNAS by attaching a hypervisor and running the replicated VMs. This provides for rapid recovery of applications and data after a disaster has occurred. Given that any ReadyNAS can replicate with any other, the secondary unit does not have to be the same model or capacity as the origin. There only needs to be sufficient capacity to support the work load and data as required. Hence the ReadyNAS should provide a sufficient platform for temporary production operations given the limited user base in effect after a disaster occurrence.

When deploying multiple ReadyNAS units in a location, there is the added benefit of live replication/migration from one unit to another. This can be configured to execute as frequently as every 2 hours or up to 24 hours. The combination of snapshots that provide the full VM context backup, offsite replications, and the ability to directly relaunch VMs on a remote ReadyNAS enables a rapid recovery scenario following a service interruption.

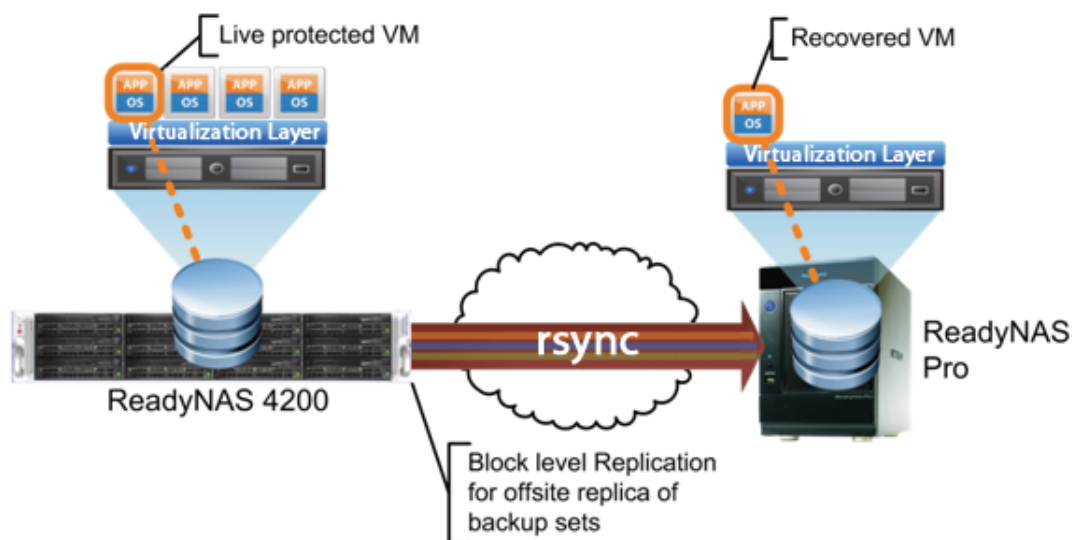


Figure 3. ReadyNAS as primary storage and a VM platform for virtual environments

ReadyNAS Protecting Remote Office/Branch Offices

ReadyNAS provides a cost effective file sharing, VM platform and DR solution for remote and branch offices. This scenario typically involves a very small number of users with a limited number of VMs, and little additional direct attached and/or networked storage. Often, users have laptops as their primary computing solution and there is minimal use of server-based applications.

The unified, storage approach of the ReadyNAS lends itself to a many-to-one backup and replication scenario with a centralized data center being the target of the branch office replications. The branch office ReadyNAS is the file server and also hosts VMs centralizing them for backup and/or replication to a central repository. In addition, 3rd party backup software can enable laptops to use the ReadyNAS as a backup to disk target, which itself will be backed up and replicated to the central repository thus providing data protection to all remote data.

A remote office or branch office DR solution usually involves a ReadyNAS in each location that replicates to a larger, central ReadyNAS. Application data, files, and laptop backups are automatically migrated to a central IT center and included in the overall corporate or service provider backup and recovery infrastructure. This combination of file sharing, snapshots, VM support, and offsite replication enables a remote office to protect its applications and data without the need for onsite storage expertise.

Hosted Disaster Recovery Services

VARs working with smaller customers or promoting their own backup and DR services can leverage the ReadyNAS platform into a hosted backup and replication service for multiple small customers, all of which can point back to a single unit at the chosen hosting site.

Hosted DR services could be provided for any of the scenarios discussed so far. The local configuration remains largely the same, but a VAR hosts the replication services and offers backup and DR strategy planning services. Since replication can be bidirectional, a VAR could choose to offer managed backup services and include rapid restore of lost or corrupted files in addition to standard DR offerings. Even the smallest of customer offices can benefit from a periodic scheduled offsite replication.

The economics for hosted DR services are favorable, especially for smaller scale customers with modest backup and replication needs. For example, DR services for 50 customers can be hosted, at a scale for only 10 active at any given moment. A ReadyNAS infrastructure scales economically to provide hosted DR services cost effectively, and profitably.

Getting Started

ReadyNAS is a flexible network storage solution that provides multiple DR services to small offices, corporate workgroups, and remote/branch offices. Whether users are addressing traditional server environments or have deployed state of the art virtual environments, the ReadyNAS platform offers choices to meet their needs. The embedded snapshot and replication technology is mature, but features user-friendly interfaces that are powerful, even in multiple unit installations. NETGEAR ReadyNAS can expand value-added offerings and grow one simple platform. Get started down the DR path by contacting your local NETGEAR representative today.

NETGEAR, the NETGEAR logo, Connect with Innovation and ReadyNAS are trademarks and/or registered trademarks of NETGEAR, Inc. and/or its subsidiaries in the United States and/or other countries. Other brand names mentioned herein are for identification purposes only and may be trademarks of their respective holder(s). Information is subject to change without notice. © 2010 NETGEAR, Inc. All rights reserved.