CONTENT PROVIDED BY

Redmond
THE INDEPENDENT VOICE OF THE MICROSOFT IT COMMUNITY

SPONSORED BY

Acronis

Asigra.
Recovery is Everything™

VEEAM
IT JUST WORKS!™

UNITRENDS

Be Prepared

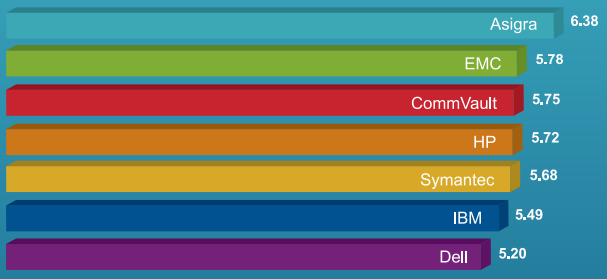
Disasters can strike at any time and in many forms. Be ready for the next one with this helpful set of articles.

1105 MEDIA

> "As customer data increased, we needed to be able to sleep at night knowing that their data was recoverable. I would categorize the Asigra team as very thorough and that's the most important quality to have when you're responsible for a customer's data."
>
> JJ Milner, Managing Director
> Global Micro Solutions
> Multi-Year Winner, Microsoft Hosting
> Solutions Partner of the Year

Cloud Backup and Recovery for Office 365

Asigra Cloud Backup™ is an agentless, multi-tenant software solution that enables the maximum in security, reliability, manageability and affordability. Asigra can help you lower your total cost of ownership with one software platform that provides data protection for physical, virtual, mobile and cloud environments with the flexibility of a private, public, and/or hybrid cloud architecture.



Asigra Sweeps 2014 TechTarget Enterprise Backup Application Comparison with Largest Margin of Victory Ever

Windows | SQL Server | Exchange | SharePoint | Office 365 | Hyper-V | Azure

Download the Executive Summary: *Enterprise Cloud Backup of Cloud-Based Applications/Platforms* or ask us about our new **Recovery License Model**.

www.asigra.com

Asigra.
Recovery is Everything™

Disaster Recovery as a Service

Microsoft has made a big bet this year that DRaaS will be a killer application for its Cloud OS and Azure service. Numerous players are making similar gambits.

BY JEFFREY SCHWARTZ

Providing the ability to recover from downtime is becoming easier and more affordable.

In today's new age of "always-on" business, prolonged downtime or even brief outages are no longer acceptable. Whether it's at a global enterprise with thousands of employees, a 200-person organization or even a small office, all are expected to have their core information systems up and running all the time. Providing the ability to recover from downtime—scheduled or unplanned—is becoming easier and more affordable thanks to a growing number of emerging enterprise-grade cloud-based Disaster Recovery-as-a-Service (DRaaS) options.

Many such DRaaS offerings, where organizations replicate snapshots of their data, system settings and applications to either a local or major cloud provider or dedicated hosting operator, have been around for some time from specialists such as SunGard or

Verizon Communications and a variety of high-end solutions. But over the past year, the sheer number and scope of options has started to amass, and many more are building out cloud-based disaster recovery service operations with varying types of capabilities, architectures and costs.

In 2014 Microsoft made a huge splash launching an extensive new portfolio of cloud-based disaster recovery options, recognizing and emphasizing disaster recovery as a key driver for its hybrid and Infrastructure-as-a-Service (IaaS) offerings. The Microsoft disaster recovery thrust came on the heels of last year's release of Windows Server 2012 R2, which included the second version of Hyper-V Replica, providing point-to-point replication of Hyper-V virtual machines (VMs) via either a LAN or WAN connection (see "Hyper-V Replica for Disaster Recovery," p. 9).

Microsoft this year made it possible to use its Microsoft Azure cloud in lieu of a secondary datacenter for disaster recovery.

Building on that, Microsoft this year made it possible to use its Microsoft Azure cloud in lieu of a secondary datacenter for disaster recovery. At the core is Azure Site Recovery, which Microsoft announced in May at its TechEd conference in Houston. Azure Site Recovery, which became generally available in October (see "First Look: Azure Site Recovery" on p. 24), is a service enabling the replication of VMs between two datacenters or from an organization's site to Azure datacenters. The service, which unlike Hyper-V Replica also supports VMware VMs and Linux servers, offers automated protection of VMs, which Microsoft backs with a service-level agreement.

The July acquisition of InMage gave Microsoft an on-premises appliance that offers real-time data capture on a continuous basis, which simultaneously performs local backups or remote replication via a single data stream. Microsoft is licensing Azure Site Recovery with the Scout technology on a per-virtual or per-physical instance basis.

At its recent TechEd conference in Barcelona, Microsoft introduced some additional capabilities including support for its Azure Automation, a runbook automation service now in preview that lets customers automate Azure Site Recovery through planned support for Windows PowerShell scripting. Microsoft sees DRaaS as a key steppingstone to

offering IaaS. DRaaS especially has appeal to customers because it delivers what for many is a much-needed capability that can be out of reach, and certainly far less expensive for those using secondary data-centers or operating co-location facilities.

Extending Azure Disaster Recovery via Cloud OS

In the same way Office 365 might not suffice for all Exchange and SharePoint users, Microsoft realizes its own Azure service won't cut it for all seeking DRaaS, either, especially those with data sovereignty requirements. As such, many Microsoft managed services and cloud hosting partners are delivering DRaaS, while some are building up to that point. One such partner is Peak 10 Inc., a hosting and managed services provider with 25 datacenters in 10 markets, whose clients include Chiquita Brands, Magazines.com, Meineke, Pergo and the PGA of America. A longtime Microsoft partner, the Charlotte, N.C.-based company has seen significant growth in its DRaaS offering this year, says Monty Blight, a vice president at Peak 10.

"Where we see people using Disaster Recovery as a Service from us are those who need a recovery time objective or a recovery point objective that's measured in minutes, rather than hours or days."

Monty Blight, Vice President, Peak 10 Inc.

"Where we see people using Disaster Recovery as a Service from us are those who need a recovery time objective [RTO] or a recovery point objective [RPO] that's measured in minutes, rather than hours or days," Blight says. "The big key component of that is the replication piece between the two."

Of course, not all organizations need, or can justify the cost, of the RTOs and RPOs of mere minutes and most commonly, it depends on the application and business function. "Where this allows the customer to have private cloud, as well as data backup to a second site, it also means you look at integrating that file-level restore, which we do for Microsoft servers all day long," Blight says. "So it integrates in with our existing backup and restore and [DRaaS] option, but also specifically on the Cloud OS it gives them a second site to ensure their data is there."

DRaaS Considerations

Indeed, while Microsoft and all of its rivals including Amazon Web Services Inc. (AWS) and VMware Inc., as well as thousands of local and regional managed services providers and hosting operators have similar designs on DRaaS. Whether or not you use all or part of the Microsoft DRaaS or Cloud OS stack, customers have no shortage of

options. At the same time, not all are created equal and IT architects need to consider numerous scenarios, requirements and capabilities, warns Enterprise Strategy Group analyst Jason Buffington.

"Providers and IT decision makers need to beware of over promising on what disaster recovery means," Buffington says. "Real disaster recovery—even in the cloud—still means I've got to have orchestration, I've got to build a sandbox so I can do testing, it means I've got to be able to define policies, so the right [VMs] come up in the right order. Based on priority and based on dependencies of those VMs, there's a lot more to it than, 'I'm going to make a copy of my VMs and put them someplace else and when something bad happens I'm going to turn them on.'"

"Providers and IT decision makers need to beware of over promising on what disaster recovery means."

—Jason Buffington, Enterprise Strategy Group analyst

Among those large enterprises using Hyper-V Relica to connect to secondary datacenters and the Azure cloud is ABM Industries Inc., the largest United States provider of facility management services ranging from HVAC repair, security and landscape maintenance with 100,000 employees and nearly $5 billion in annual revenues. Andre Garcia, ABM's assistant vice president of global technology, referred to the disaster recovery scenario during a panel session on Hyper-V migration at the August TechMentor Redmond conference, which, like Redmond magazine is produced by 1105 Media Inc.

"Hyper-V Replica is just a feature of Hyper-V that's on by default—you just have to right-click and tell VMM [Virtual Machine Manager] what the target is for that source," Garcia said during the panel discussion. "It's a phenomenal capability," added panel participant Matt McSpirit, a Microsoft technical product manager focused on Hyper-V. "It has enabled organizations to replicate changes up to every five minutes, between Site A and B. It's well-received, with a PowerShell layer for automating it."

One shortcoming of Hyper-V Replica is that it's synchronous. Microsoft has said it's developing an answer to that with a new tool called Storage Replica (see more **bit.ly/1tDpmyH**).

Alternative Services Emerge

Yet numerous other software and services providers—many point out they're Microsoft partners—say organizations need better automation and replications than Hyper-V replica can offer. Many of them point to

better recovery times, links to multiple clouds and faster continuous data protection (CDP), compression and data deduplication algorithms. Most dismiss Microsoft Hyper-V Replica as a suitable base-level replication mechanism for creating Windows Server Hyper-V clusters, but not sufficient for providing complete DRaaS.

There's no shortage of those who have stepped up their DRaaS offerings and market presence this year. Among them in various stated of delivering new DRaaS capabilities are Acronis International GmbH, ArcServe (spun off from CA Technologies), Asigra Inc., Axcient Inc., Dell Inc. (AppAssure), Hewlett-Packard Co. (via its Helion cloud platform), Nasuni Corp., Symantec Corp., Vision Solutions Inc., Unitrends, Veeam Software and Zerto, while CommVault is said to have new DRaaS capabilities in the works.

"Hyper-V Replica definitely has a place for the lower tier workloads."

–Tim Laplante, senior product director, Vision Solutions Inc.

"Hyper-V Replica definitely has a place for the lower tier workloads," says Tim Laplante, a senior product director at Vision Solutions Inc., supplier of DoubleTake. "But where you need true high availability or you need to replicate it to something other than Hyper-V, you're going to need a solution like ours, where you need the real time and the flexibility from a target perspective."

Laplante points to Peak 10 as a provider that subscribes to that model. Peak 10's Blight says while using Hyper-V Replica is suitable in certain scenarios is suitable, in others he sees the need for third-party solutions, notably Double Take and Zerto.

"The customer who needs DoubleTake requires real-time replication," Blight says. In cases where CDP is necessary, Peak 10 has also been working with Zerto, whose namesake software has long-offered that capability for VMware environments and last month gained Hyper-V support.

Many providers of backup software are making big pushes into DRaaS. Veeam, the rapidly growing provider of VM backup and disaster recovery software for midsize organizations, in October kicked off a major push into DRaaS, adding a component to its newly branded suite called Veeam Backup and Replication v8. A key new component in its new release, Cloud Connect, offers an interface that lets users search a network of partner cloud providers and

MSPs. The initial Cloud Connect supports just backup and recovery. Next year providers will also be able to deliver DRaaS using Cloud Connect.

"We believe that next year will be the year where disaster in the cloud will start to become mainstream," says Veeam CEO Ratmir Timashev, "and we will be one of the driving forces for that, because we have a better license base and we provide this very easy out-of-the-box experience for end customers and for our service providers."

The MSP Azure Connection

Veeam is also enabling its MSP partners to use the back-end services of Azure. The company has made Cloud Connect available in the new Azure Marketplace. "Veeam cloud providers who want to offer Veeam Cloud Connect [can] leverage Azure to provide the underlying core infrastructure–network, compute and storage in the form of VMs,"says Rick Vanover, a Veeam product strategy specialist. Selecting the Veeam Cloud Connect option in the [Azure] Marketplace will let that Veeam partner run the Cloud Connect infrastructure in Azure."

Not all DRaaS providers see the benefits of using a larger cloud provider. If you're not using DRaaS yet, you're not alone.

Unlike Veeam, Unitrends operates its own cloud and argues it offers higher service levels than what's available by larger cloud services like Amazon EC2/S3 and Azure. In addition to integrating its on-premises appliance with its cloud, Unitrends offers its own DRaaS and touts a tool called Reliable DR, which offers governance and compliance auditing. The company says its DRaaS has grown 180 percent this year to hundreds of customers. "They have the advantage of our software to build out similar services that we have," says Ubo Guha, Unitrends vice president of product management. Unitrends is still considering whether to forge ties with Azure, Amazon or another major cloud network.

Not all DRaaS providers see the benefits of using a larger cloud provider. "Public clouds are generally not purpose built, so they're good at many things, not great at any one application layer," says Justin Moore, CEO of Axcient, which provides a turnkey replication appliance and runs its own multi-petabyte cloud for DRaaS. "If you think of disaster recovery as a service, it's more of an application layer offering than it is an infrastructure."

The City of Williamsburg in Virginia is among those who have deployed a DRaaS solution using the Axcient service, where it backs up 10TB of data including its Novell GroupWise server, SQL Server databases and file systems, all running on 22 servers tied to VMware-based VMs. The replication is performed overnight, meaning in a worst-case scenario, the city's data would be 24 hours old. "We're pretty small so that's a pretty good recovery time objective," says the city's IT manager Mark Barham. "I could knock it down to 30 minutes if I wanted to."

The Outdoor Group LLC, which supplies sporting goods gear—mainly high-end archery equipment—has started using the Veeam Cloud Connect tool through DR provider Offsite Data Sync to replicate its Exchange e-mail system, SQL Server databases, and various application servers. "If we lose that information we're basically starting over from scratch," says IT Director Jim Klossner.

If you're not using DRaaS yet, you're not alone.

TBG Partners, a landscape architecture firm uses Nasuni's replication service. With the Nasuni appliances, CTO Greg Nichols says his company can replicate large CAD files that could be gigabytes in size each. Nasuni offers customers a choice of AWS or Azure to host their backed-up data. Nichols says data is backed up more frequently for the firm's architects. "Having it backed up every five minutes is great for our users, because they literally don't lose anything," he says.

Buyer Beware

Gartner Inc. analyst Pushan Rinnen warns customers that Backup as a Service shouldn't be confused with DRaaS, even as many of the same companies offer both. "Disaster recovery involves not just the bits of the data, a copy of the storage part, but a lot of the business processes in the servers, applications and the consistency of the data," she says. "It's a lot more complex than backup."

If you're not using DRaaS yet, you're not alone. Many of these services are in their evolutionary state, Rinnen says. "We are definitely seeing more implementations of Disaster Recovery as a Service," she says. "But we're still very early at the beginning stage." R

Jeffrey Schwartz is editor of Redmond *magazine.*

VEEAM
IT JUST WORKS!™

AVAILABILITY™
for the Modern Data Center

High-Speed Recovery

Data Loss Avoidance

Verified Protection

Leveraged Data

Complete Visibility

NEW Veeam Availability Suite v8
Download FREE trial version

Hyper-V Replica for Disaster Recovery

The replication feature Microsoft introduced in Windows Server 2012 provides business continuity. Though no substitute for failover clustering, it's an affordable option.

BY BRIEN M. POSEY

Hyper-V offers a replica feature that's well suited for helping smaller organizations improve their disaster readiness.

Although many small and midsize businesses run their workloads on virtualized servers, they haven't been able to take advantage of the fault tolerant capabilities of virtualization such as failover clustering. The licensing and hardware costs and technical complexity involved in building a clustered Hyper-V deployment tend to put failover clustering out of reach for smaller organizations. Fortunately, Hyper-V offers a replica feature that's well suited for helping smaller organizations improve their disaster readiness.

Appropriately called Hyper-V Replica, Microsoft introduced it with Windows Server 2012 R2 and upgraded it in the subsequent release. While it provides replication designed to ensure business continuity, Hyper-V Replica is not a substitute for failover clustering. If your

organization has the budget to build a clustered Hyper-V deployment, you should definitely do so. Although there are similarities between replication and failover clustering, failover clustering is the preferred method for protecting your virtual machines (VMs).

Of course, that isn't to say the Hyper-V Replica feature is inadequate—quite the contrary. I use Hyper-V Replica to protect my own VMs. I recommend the use of failover clustering whenever possible because a failover cluster's job is to make sure critical workloads never go offline. Replication won't guarantee that your VMs stay running in the event of a disaster, but it will give you at least one "spare copy" of your VMs, which you can launch at a moment's notice.

The Hyper-V Replica feature is based on the idea of asynchronously replicating a virtual disk from a primary site to a replica site.

The Hyper-V Replica feature is based on the idea of asynchronously replicating a virtual disk from a primary site to a replica site. Although Microsoft refers to the source and target in terms of sites, it's important not to confuse the concept with Active Directory sites or geographic sites. In my own organization, for instance, my primary and replica "sites" exist within the same rack and on the same network segment.

The replication process occurs at the virtual hard disk level on an asynchronous basis. Once the initial copy process has been completed, replication occurs on a scheduled basis. In the version of Hyper-V Replica delivered with Windows Server 2012 R2, it's now possible for administrators to adjust the replication frequency. Replication can be scheduled to occur at 30-second, five-minute or 15-minute intervals. Intervals of 30 seconds do the best job of keeping the replica up-to-date, but aren't always appropriate. If the primary server is heavily utilized or if there's a slow link between the primary and the replica servers, then a longer duration replication frequency might work better.

Another improvement is the addition of Hyper-V Extended Replication. Extended Replication allows for the creation of a secondary replica. The most common use for this feature involves placing one replica within the local datacenter (so that it's easily accessible) and placing the secondary replica in a remote location (so that it's protected against datacenter-level disasters).

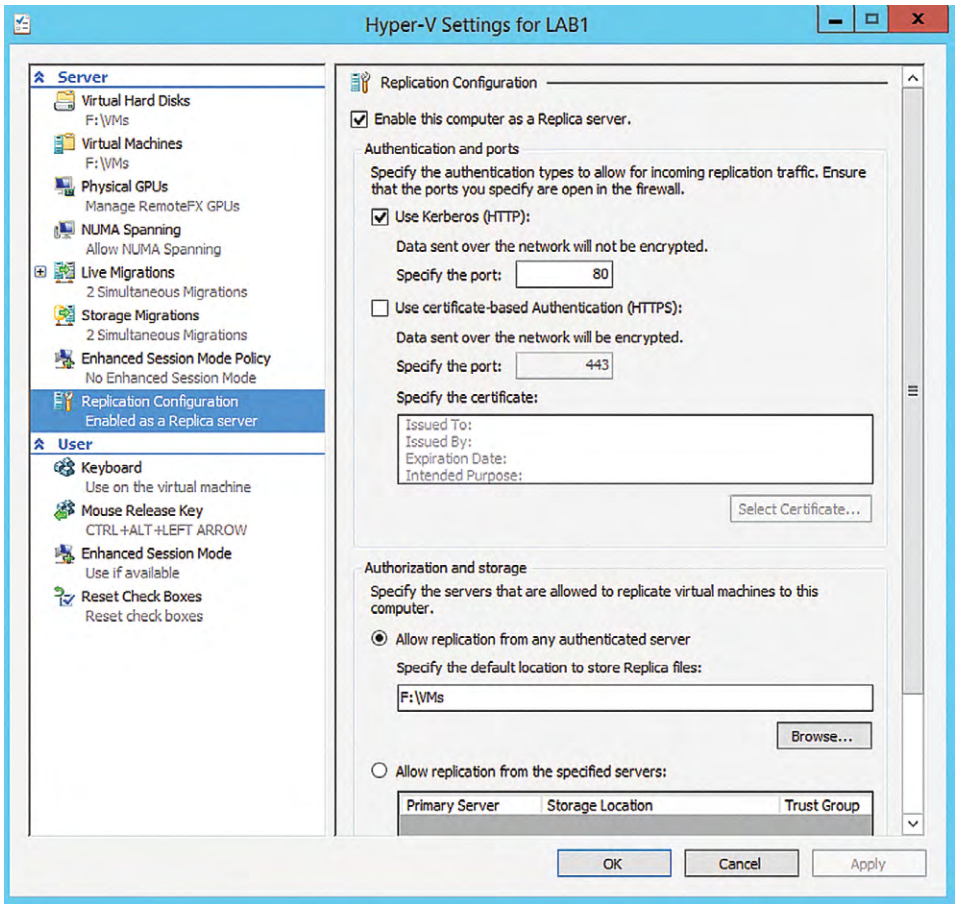


Figure 1. *Select the Replica Configuration container.*

An important consideration is the authentication type that's used by the replication process.

Planning Considerations

First, the server that will store your replica doesn't need to be 100 percent identical to your source server, but it needs to be capable of hosting your VMs if necessary. As such, you'll need to make sure the replica server has adequate hardware resources to ensure a good UX in the event that it ever has to be put into use.

Another important consideration is the authentication type that's used by the replication process. By default the replication process is based around the use of Kerberos and the HTTP protocol. If you require encryption, however, you might be better off using certificate-based authentication, which is based on HTTPS.

You'll also need to consider the initial synchronization process. Normally, you should be able to perform the initial synchronization process across the network. In the case of excessively large VMs, you're often better off using removable media to create the initial replica.

In addition, you'll need to consider other aspects of the replication process, such as the most appropriate frequency and whether you'll require extended replication.

Enabling Hyper-V Replication

The process of enabling Hyper-V replication involves performing various tasks on both the source server (the primary site) and the destination server (the replica site). Incidentally, the focus here is on Hyper-V replication in terms of a source server and a destination server, but you can replicate a VM to or from a cluster, or even between clusters so long as the Replication Broker is installed.

The process of enabling Hyper-V replication involves performing various tasks on both the source server and the destination server.

The destination server must be configured first. Open the Hyper-V Manager, select the listing for the destination host server and then click on the Hyper-V Settings link, found in the Actions pane. When the Host Server Settings dialog box opens, select the Replica Configuration container (see **Figure 1,** p. 11).

Next, select the Enable this Computer as a Replica Server checkbox. You'll also need to select the type of authentication you want to use: allowing replication from any authorized server or specifying a list of Hyper-V servers from which you want to allow replication. Finally, click the Browse button and specify the location where you want to store the VMs. Click OK to complete the process. You might receive a warning message saying you need to configure your firewall to allow replication traffic.

The next thing you need to do is to open the Hyper-V Manager on the source server. Next, right click on the VM you want to replicate and select the Enable Replication command from the shortcut menu. You can replicate multiple VMs, but you'll need to enable replication separately for each VM.

At this point, Windows will launch the Enable Replication Wizard. Click Next to bypass the wizard's Welcome screen and you'll see a screen prompting you to enter the name of the replica server. Enter your destination server's name and click Next. When prompted to enter an authentication type, make sure to specify the same authentication method you used on the destination server and click Next.

You'll be asked if you want to compress the data sent across the network. Compression reduces bandwidth consumption, but slightly increases CPU utilization. It's usually a good idea to use compression. Make your selection and click Next.

The next screen you'll see asks you to specify the virtual hard disks you want to replicate. Remember, replication works on a per-virtual hard disk (not a per-VM) basis. Click Next and you'll be asked to specify your replication frequency. After doing so, click Next.

The following screen asks you to choose the number of recovery points you want to store for the VM. Creating recovery points allows you to revert the replica to an earlier point in time. Windows Server 2012 R2 allows up to 24 hours' worth of recovery points to be maintained (the previous limit was 15 hours). It's worth noting that the replica's storage requirements increase as you add recovery points.

It's worth noting that the replica's storage requirements increase as you add recovery points.

Click Next and you'll be prompted to select the method you want to use for the initial synchronization process. After doing so, click Next. Assuming you're synchronizing across the network, you'll be asked when you'd like the replication process to begin. Make your selection and click Next. You should now see a summary screen displaying the replication options you've chosen. Take a moment to make sure

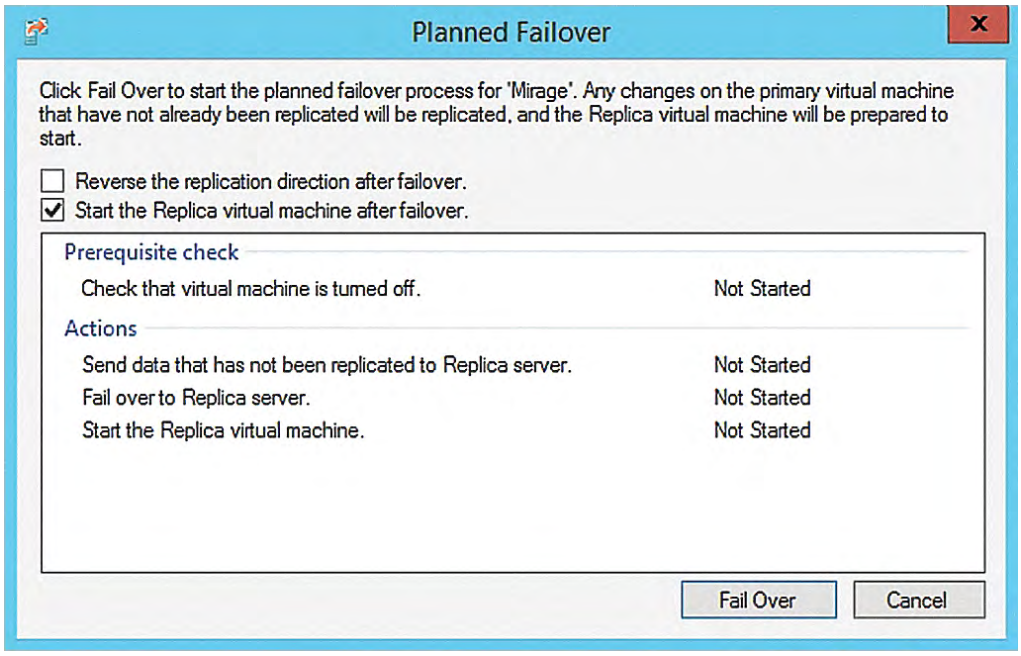


Figure 2. *The Planned Failover dialog box.*

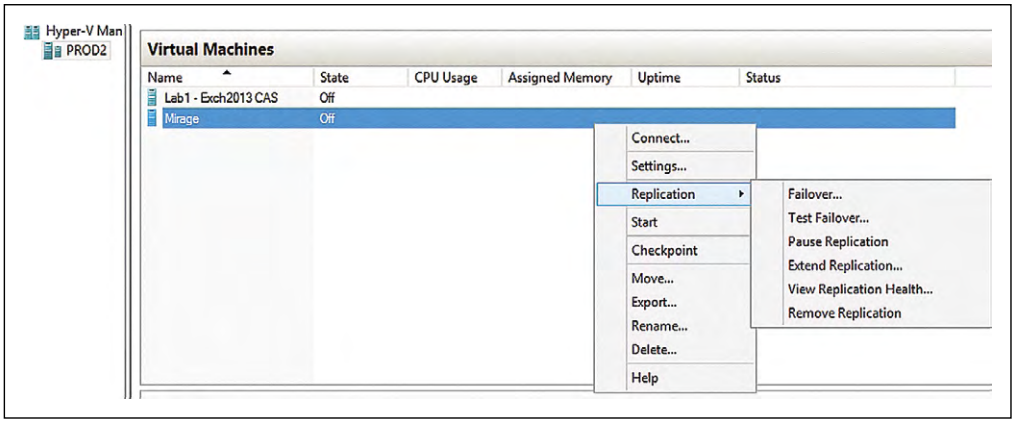


Figure 3. *The Replication | Failover commands from the shortcut menu when right-clicking the VM replica to perform an unplanned failover.*

A planned failover is useful in situations in which you need to take the primary host offline for maintenance.

everything is correct and click Finish. When you do, the VM Status should change to Initial Replication.

Replica Failover

As previously noted, replicas exist for disaster recovery purposes. As such, you can perform a planned failover or an unplanned failover. You can also perform a test failover.

A planned failover is useful in situations in which you need to take the primary host offline for maintenance. To do a planned failover, however, you need to first power down the VMs being replicated.

To perform a planned failover, right-click on the VM and select the Replication | Planned Failover commands from the shortcut menu. You'll see the dialog box in **Figure 2** (p. 13). You can complete the failover by simply clicking on the Fail Over button. However, it's usually a good idea to select the Reverse the Replication Direction After Failover checkbox first. This checkbox causes the source VM to become the replica and the replica to become the primary.

You can safely perform a planned failover at any time. An unplanned failover should only be performed in the event that your primary VM has suffered a catastrophic failure. The reason for this is that an unplanned failover does not perform a synchronization as part of the failover process. Consequently, any data not already synchronized will be lost. The amount of data lost depends on the length of your

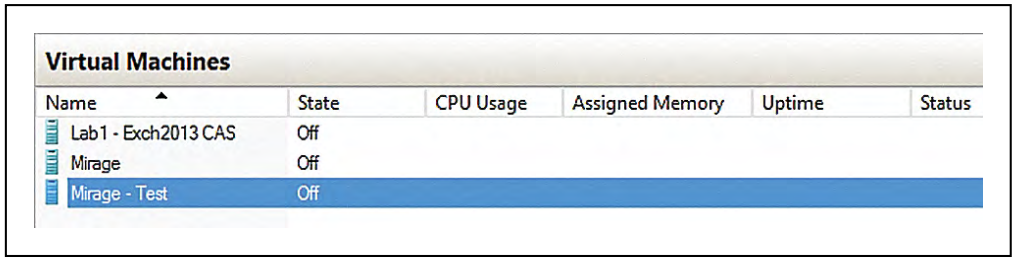


Figure 4. *The test virtual machine.*

replication cycle and the volume of data that was added to the primary VM since the last successful replication cycle.

To perform an unplanned failover, open the Hyper-V Manager on the server that contains your VM replica.

To perform an unplanned failover, open the Hyper-V Manager on the server that contains your VM replica. Right-click on the replica and select the Replication | Failover commands from the shortcut menu (see **Figure 3**, p. 14). Next, choose the recovery point that you want to use for the failover and then click the Failover button.

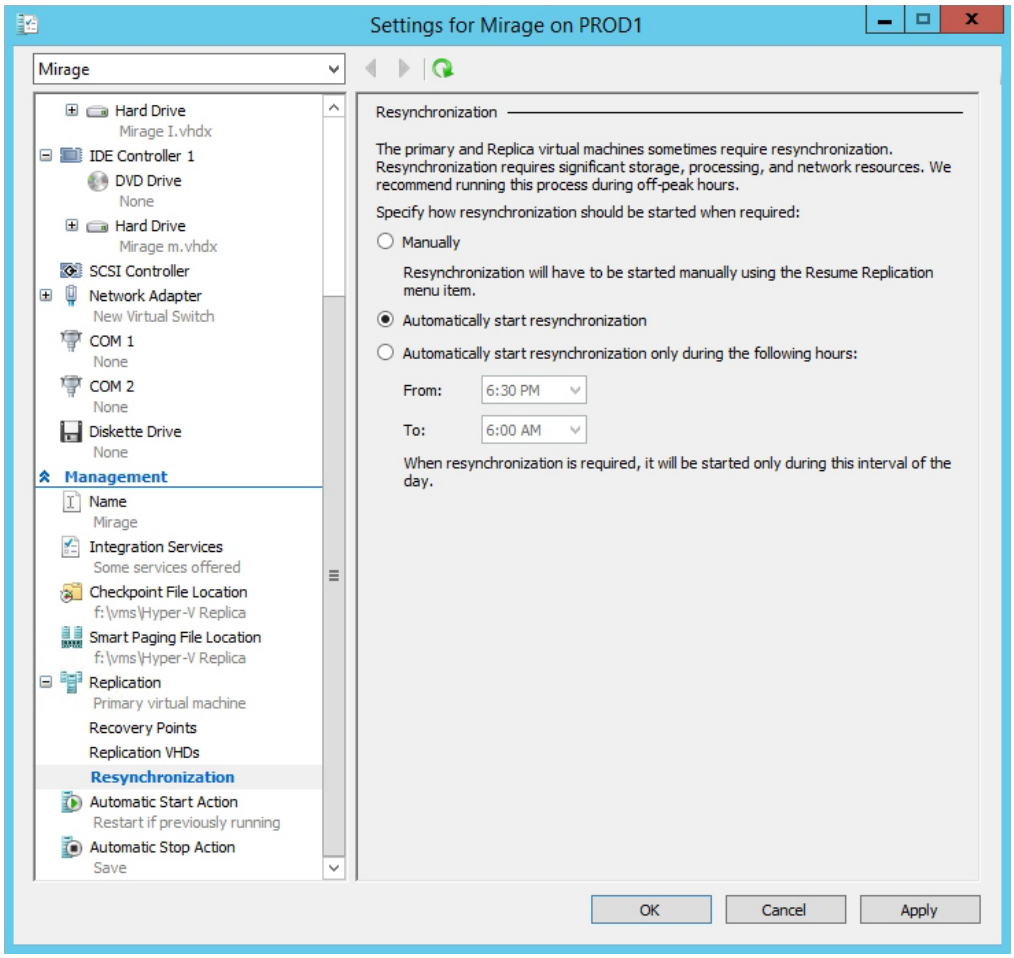


Figure 5. *It's a good idea to enable automatic resynchronization.*

It's a good idea to perform a test failover. A test failover doesn't actually result in a failover. Instead, the process creates a brand-new test VM. This test VM lacks network connectivity, so it can be safely powered on and tested. There's a VM named Mirage-Test (see **Figure 4**, p. 15), which is a test VM.

You can perform a test failover by going to the replica server, right-clicking on the VM, and selecting the Replication | Test Failover commands from the shortcut menu. Upon doing so, you'll be asked to select the recovery point you want to test. Make your selection and click the Test Failover button.

If you're going to use the replication feature, I strongly recommend enabling the automatic resynchronization of replicas.

When you're done with your tests, right-click on the destination VM (not the test VM) and select the Replication | Stop Test Failover commands from the shortcut menu. This will cause the test VM to be deleted and everything will be put back to normal.

Replica Resynchronization

If you're going to use the replication feature, I strongly recommend enabling the automatic resynchronization of replicas (see **Figure 5**, p. 15). Replicas occasionally fall out of sync, and the resynchronization feature can fix the problem whenever necessary. You can access this feature by right-clicking on your VM and selecting the Settings command from the shortcut menu. When the Settings dialog box appears, expand the Replication container to reveal the Resynchronization container. You can choose to manually resynchronize, automatically resynchronize or automatically resynchronize during a scheduled time.

The Hyper-V replica feature is relatively easy to use, but there are loads of features not covered here, which you should explore. R

Brien M. Posey is a seven-time Microsoft MVP with more than two decades of IT experience. He's written thousands of articles and several dozen books on a wide variety of IT topics. Visit his Web site at brienposey.com.

SIMPLE.
AFFORDABLE.
SCALABLE.

PROTECT YOUR UNIQUE MIX of data center assets with Unitrends Recovery-Series appliances. All in one data protection, instant recovery, and cloud recovery backed by a customer support team that consistently achieves a 98% satisfaction rating.

OUR INTEGRATED APPLIANCE MODELS:

Support from 2TB to 97TB of raw storage, with 4GB to 256GB memory and 2 to 16 CPU cores.

Offer unified compute protection for over 100 versions of applications, operating systems, servers, and storage.

Perform one-pass dissimilar bare metal as well as granular file-level backup.

Support cloud-empowered disaster recovery and business continuity your way.

LEARN MORE TODAY.
www.unitrends.com
1.866.359.5411

UNITRENDS

"160 POUNDS OF BACKUP AWESOMENESS."

- CLANDIS S. | Lincoln Memorial Recovery-943 Customer

7 DRaaS Platforms Gaining Speed

There's no shortage of software, hardware and cloud providers adding Disaster Recovery as a Service (DRaaS) if Hyper-V Replica isn't enough for your requirements.

BY JEFFREY SCHWARTZ

If Microsoft's Hyper-V Replica doesn't meet your service-level requirements, there's no shortage of providers of software, hardware and appliances that suppliers are making available for cloud- based Disaster Recovery as a Service (DRaaS). Many are offered as appliances, others as pure software and services solutions.

Some suppliers run their own cloud services.

Some suppliers run their own cloud services, others are in the process of enabling partner networks of local and regional managed services and hosting providers to deliver those services. A number now also offer the option to use both local services providers and large ones such as Amazon Web Services (AWS) and Microsoft Azure. Others are still looking into doing so. Here are seven providers that have recently updated their offerings:

DRaaS Coming to Veeam Availability Suite in 2015 via Cloud Connect

The newly released Veeam Software Data Availability Suite v8 looks to enable customers who have used its virtual machine-focused backup and recovery software to implement disaster and recovery capabilities via secondary datacenters or using a cloud services provider. CEO Ratmir Timashev says that Veeam is on pace to post $500 million in booked revenue (non GAAP) this year and is aiming to double that to $1 billion by 2018. To get there, Timashev sees the growing DRaaS business as a key catalyst of that growth.

CEO Ratmir Timashev says Veeam can reach those fast-growth goals without deviating from its core mission of protecting virtual datacenters.

Timashev says Veeam can reach those fast-growth goals without deviating from its core mission of protecting virtual datacenters. The new Data Availability Suite v8 incorporates the company's new Cloud Connect interface that will let customers choose from a growing network of partners that are building cloud-based and hosted backup and disaster recovery services.

Released last month, the Cloud Connect component initially only supports backup and recovery with DRaaS replication promised early next year, Timashev says. "From the user perspective, they are just going to see in the interface, 'Do you want to also backup up to cloud?,' and then they can select, 'Yes,' and then they can go directly to our Web site for the services provider they want to use. We have a simple registration and certification process for them to become a services provider who is using the Cloud Connect. So customers will be able to select in different countries the services providers in their cities."

Because Veeam Cloud Connect just became available, the company has only formally announced a handful of providers offering the service. They Include Cirrity LLC, iLand, NewCloud Networks, OffisteDataSync and Phoenix NAP. Veeam says it aims to have 1,500 services providers available in the coming year.

The new v8 suite offers a bevy of other features including what it calls "Explorers" that can now protect Microsoft Active Directory and SQL Server, and provides extended support for Exchange Server and SharePoint. Also added is extended WAN acceleration introduced in

the last release to cover replication and a feature called Backup IO, which adds intelligent load balancing.

Unitrends New Offering Links Appliances and Cloud Service

The new Unitrends DRaaS offering uses the company's own cloud network, which it believes offers higher service levels than larger cloud services providers such as AWS Inc., Microsoft and Google. Though the company hasn't ruled out partnering with such players or others in the future for certain capability, the DRaaS offering lets customers use its appliances to conduct on-site backups of servers and virtual machines (VMs) and utilize its continuous data replication technology for data, systems and applications to the company's No Limits Cloud service, which the company says offers 24x7 telephone services and the use of its newly acquired optional Reliable DR disaster recovery testing tool to meet compliance and governance requirements.

"We provide what we call deep virtualization, meaning we can go into the application that sits on the virtual machine."

–Ubo Guha, vice president of product management, Unitrends

Either live VMs or physical servers are spun up in real time to the cloud, providing recovery of those systems in the event of unplanned downtime or a disaster. On-premises appliances range in configuration from 1TB to 97TB and the company also offers software-based virtual appliances for instant recovery of both physical and VMs.

"We take it one step further and provide what we call deep virtualization, meaning we can go into the application that sits on the virtual machine," says Ubo Guha, Unitrends vice president of product management. "There may be an application like Exchange or custom apps that need to have a lot more deeper management of the operating system, the application, and you might want to adjust things."

Vision Solutions Adds DRaaS to DoubleTake

The new DoubleTake 7.1, released last month from Vision Solutions Inc., dons a number of improved migration and high-availability features, but also provides disaster recovery for Windows hybrid cloud environments. It's suited for DRaaS, thanks to a new metered usage feature available for cloud and managed services providers deploying the product.

DoubleTake 7.1 is also now fully API-enabled and designed with full server data replication and is container-based rather than

volume-based. It supports the new Microsoft virtual hard drive format VHDX and its Volume Shadow Copy Service (VSS), says Tim Laplante, director of product strategy at Vision Solutions.

"This provides more granular level of control and gives you that near CDP [continuous data protection), which is nice because it gives you the best of both worlds," Laplante says. "If there's a disaster and you need to execute your DR plan, it gives you the option at that point to say, 'Do I need to go back to that exact point in time, or do I need to go back to 15 minutes ago because it was really just a virus or data corruption that happened, so I need to step back for a couple of minutes to the point that happened before then?"

Zerto has recently entered the Hyper-V world.

Besides the metered usage, it's suited for DRaaS in that the DoubleTake 7.1 repository can replicate both physical machines and VMs on-premises to another datacenter, private cloud or public cloud. Likewise, recovery service can be anywhere in the physical, virtual and cloud mix, as well. Administrators can specify discrete repository server targets, so customers know exactly where a specific system and data is, which should appeal to those who have sovereignty requirements. "It's not that your data is in multiple zones," Laplante says. "You know exactly where that data is when you need it for compliance purposes."

With the new disaster recovery feature in DoubleTake, LaPlante says Vision Solutions will step up working with services providers to offer DRaaS. "It's a huge piece of where we see our growth," he says.

Zerto Virtual Replication Now Supports Hyper-V

Zerto, a 4-year-old company with headquarters in Israel and the United States that provides disaster recovery and replication software, until now has a following among VMware Inc. shops. The company has recently entered the Hyper-V world. The Zerto Virtual Replication now supports replication of Hyper-V hypervisors to other Hyper-V targets, as well as to vSphere and vice versa.

In short, the company says its CDP-based replication tool is now hypervisor-agnostic. Gil Levonai, the company's president of marketing, says its software offers recovery point objectives (RPOs) of seconds, and said it can provide consistent recovery of multiple VM applications. It doesn't use snapshots, just CDP, automatically

orchestrates disaster recovery processes ensuring the consistency of applications and data, and generates reports.

"We took real hard enterprise-class replications from storage and moved it into the hypervisor," Levonai says. "You don't have to worry about where the VM is and you don't care about where the data is. You can move it between storage. We are agnostic to storage because we are replicating virtual objects, which can be VMs or volumes."

Dell Combines Backup and DRaaS in New AppAssure Suite

Dell is offering AppAssure as part of a new data protection that includes NetVault Backup and vRanger backup and recovery offerings.

Dell Inc. was one of the earliest players to offer DRaaS to enterprises and earlier this year said it has more than 1,000 managed services providers (MSPs) offering its AppAssure replication software. The latest release, AppAssure 5.4, offers multi-target and multi-hop replication, which the company claims makes it suited for multi-tier disaster recovery.

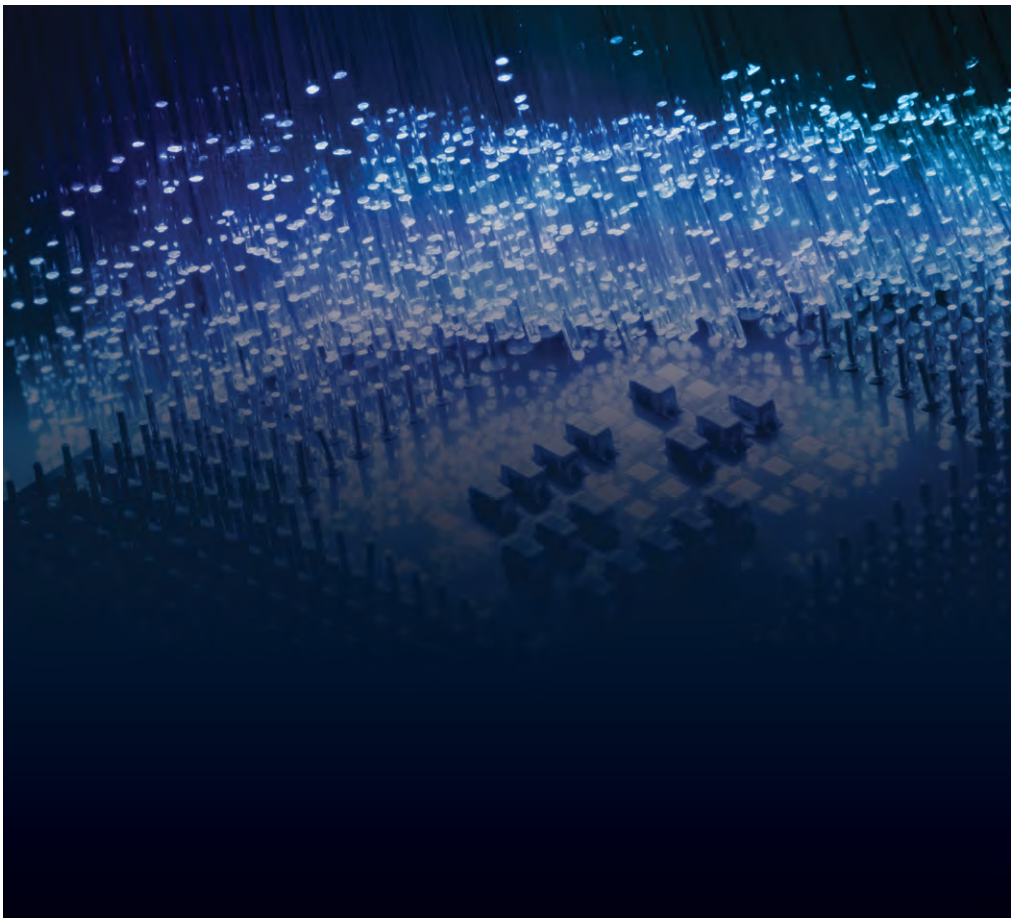
AppAssure 5.4 also lets customers set multiple data retention policies both for on-premises and off-site cloud and MSP facilities. Customers can customize replication schedules for each target, enabling them to throttle when needed and restrict speed in bandwidth-limited situations.

Dell is offering AppAssure as part of a new data protection that includes NetVault Backup and vRanger backup and recovery offerings. The company is also now offering a capacity-licensing model with a range from 1TB going as high as 250TB of data.

Acronis Enters DRaaS with nScale Deal

Known for its protection of Windows physical and virtual file server data protection wares, including specialty versions for SharePoint, Exchange, SQL Server and VMware environments, Acronis International GmbH in September jumped into the DRaaS mix with the acquisition of San Francisco-based nScaled.

Acronis says users of its Hosted Backup as a Service offering will be able to use nScale to extend that into a cloud-based disaster recovery offering. The company will enable its partners to offer the nSCaled DRaaS offering, which is designed to enable remote and



Nasuni customers can now choose which provider they want their data replicated to.

local sites to failover via the cloud to ensure recovery within minutes of an outage.

Nasuni Adds Azure to DRaaS

Until recently Nasuni Corp. has relied on AWS as the cloud provider for its DRaaS offering, now the company has added the Microsoft Azure service as an option. Customers can now choose which provider they want their data replicated to, or if they prefer, can use both for contingency.

The latest version of its offering was released this summer. It includes the 6.0 release, which the company says adds file data virtulization that separates file data from storage hardware. It adds global file locking to utilize cloud storage architectures. With it is the new Nasuni Filer NF-100 appliance, the company says service is suited for providing recovery of blocks of data including CAD and BIM files. R

Jeffrey Schwartz is editor of Redmond *magazine.*

Acronis

Backup FREE FOR DUMMIES®

A Wiley Brand

Download the e-book at
www.acronis.com/dummies

Learn:

- Answers to common questions about backup and recovery.
- Ten tips for easier backup and recovery.
- How to address the modern data protection challenges caused by virtualization, the cloud and data growth.

First Look:

Microsoft Azure Site Recovery

Hyper-V virtual machine protection in a private cloud or the Azure cloud is simplified with the new replication and recovery service.

BY JEFFREY SCHWARTZ

Nightly backups have largely become inadequate.

The best way to truly protect your data is to have at least three copies of it. First, there's the original copy—the live data, of course. Next, you need a backup copy of the data that you can quickly and easily restore. The third copy is the alternate backup that resides outside your datacenter. Once upon a time you could fulfill these requirements by writing a nightly backup to redundant tapes and keep one tape on-site and ship the copy off-site for safe keeping.

This tried-and-true backup technique is now outdated. Nightly backups have largely become inadequate. Organizations have come to expect near-real-time data protection. In the scramble to provide top-notch protection in the virtual datacenter, a number of competing solutions have evolved. Even Microsoft provides several different ways of protecting Hyper-V virtual machines (VMs).

At first glance, one of Microsoft's solutions would seem to be ideal: Hyper-V Extended Replication. If you aren't familiar with Hyper-V Extended Replication, it's a feature that was introduced with Windows Server 2012 R2 that allows you to create two separate replicas of a VM. One of these replicas can reside in the local datacenter, while the other can reside outside the datacenter. As such, the Hyper-V Extended Replication feature provides near-real-time protection, while also meeting the requirements of my three-copy rule. When you consider that Hyper-V replicas can be configured to provide point-in-time rollback capabilities, Hyper-V replicas appears to be an ideal solution.

While native Hyper-V replication is designed to replicate individual VMs, Azure Site Recovery is focused on private cloud replication.

There's just one problem with protecting your VMs using Hyper-V Extended Replication. The feature was designed for small and midsize businesses and simply doesn't scale well enough to make it a viable option for protecting large, enterprise-class organizations. So what's a company to do?

Enter Microsoft Azure Site Recovery—a new disaster recovery feature in Azure that can replicate Hyper-V VMs in a way that can provide better scalability.

While native Hyper-V replication is designed to replicate individual VMs (or even individual virtual hard disks), Azure Site Recovery is focused on private cloud replication. In other words, if you have a System Center Virtual Machine Manager private cloud, you can replicate your Hyper-V VMs to another private cloud that's running in another datacenter. As an alternative, you can replicate VMs to Azure.

Although enabling protection for VMs involves a little bit of work up front, the process is surprisingly straightforward. The key to making the process work is ensuring the certificates are configured correctly. The certificates are used to positively identify your Virtual Machine Manager server to Azure.

Creating a Self-Signed Certificate

In order to use Azure Site Recovery, you need to generate a certificate. A self-signed certificate will work fine. There are a few different ways of generating the necessary certificate, but Microsoft recommends using a tool found in the Windows SDK for Windows 8.1 called MakeCert.exe (**bit.ly/1DrOjTG**). The SDK has a lot of

different components, but the only component you have to install is the Windows Software Development Kit.

After installing the MakeCert utility, open an elevated command-prompt window and navigate to C:\Program Files (x86)\Windows Kits\8.1\Bin\x64 and run the following command:

```
makecert.exe -r -pe -n CN=AzureBackup -ss my
-sr localmachine -eku 1.3.6.1.5.5.7.3.2 -len 2048
-e 01/01/2016 AzureBackup.cer
```

Azure is very picky about the way you create the self-signed certificate. If you deviate from the command here, MakeCert may tell you that you've entered too many parameters, or you could end up creating a certificate that Azure won't accept. Both are common problems you want to avoid, so be sure to correctly type the command.

While native Hyper-V replication is designed to replicate individual VMs (or even individual virtual hard disks), Azure Site Recovery is focused on private cloud replication.

Importing the Certificate

Now that the self signed-certificate has been created, you need to import it into the computer on which Virtual Machine Manager is running. To do so, enter the Microsoft Management Console (MMC) command at the server's Run prompt. Then, choose the Add/Remove Snap-in command from the shortcut menu. When the list of snap-ins appears, choose the Certificates option and click Add. When prompted, make sure to choose the Computer Account option, and then click Next. After that, choose the Local Computer option and click Finish, followed by OK.

Right-click on the Personal container and select the All Tasks | Import commands from the shortcut menus. This will cause Windows to launch the Certificate Import Wizard. Click Next, and then browse to and select the certificate you created earlier. Now, complete the wizard. When you're prompted to specify the certificate store, be sure to put the certificate in the Personal store.

Exporting the Certificate

Now you need to export the certificate in PFX format. To do so, navigate through the Certificates console tree to Certificates (Local Computer) | Personal | Certificates. Right-click on the certificate and select the All Tasks | Export commands from the shortcut menus.

You need to import the certificate on your Virtual Machine Manager servers.

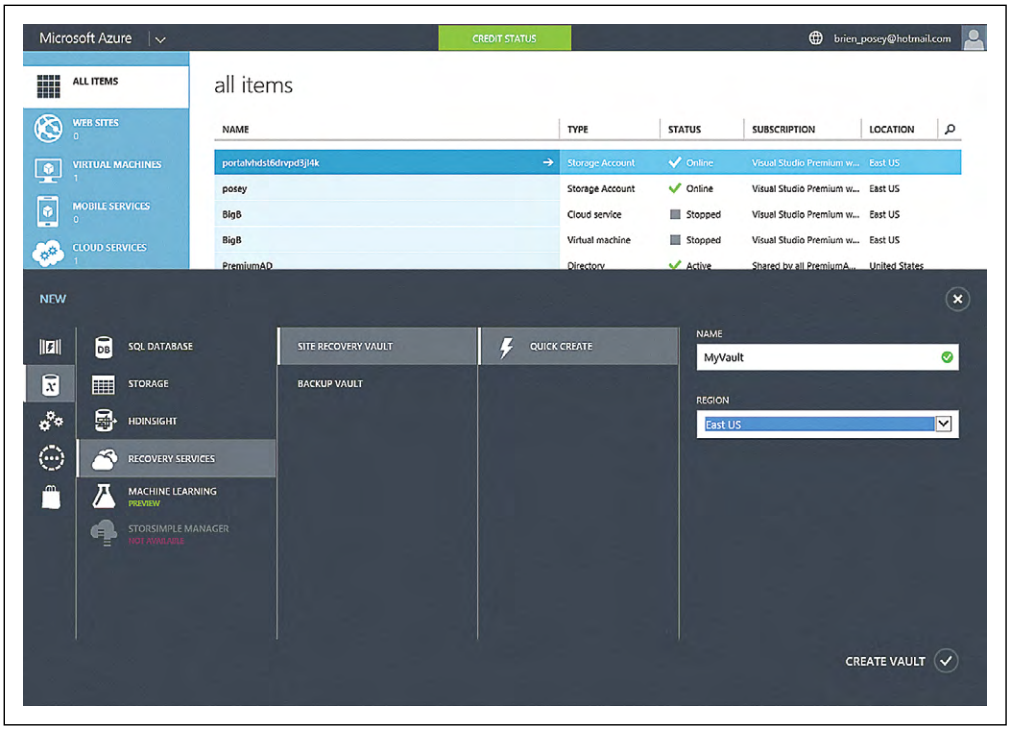


Figure 1. *Creating a Site Recovery Vault in the Microsoft*

This will cause Windows to launch the Certificate Export Wizard. Click Next and you'll be asked if you want to export the private key. Choose Yes and click Next. Make sure the wizard is set to export the certificate in PFX format and then click Next. On the following screen, you must enter and confirm a password that can be used to encrypt the private key. Click Next and you'll be prompted for a path and filename to use for the exported certificate. Click Next, followed by Finish to complete the process.

Now you need to import the certificate on your Virtual Machine Manager servers. If you only have a single Virtual Machine Manager server and you already imported the certificate on that server, then you can skip this step. Otherwise, open the Certificates console on your Virtual Machine Manager server and import the PFX file you just created.

Create a Site Recovery Vault

The next step in the process is to create a Site Recovery Vault. You'll need to log in to the Azure Management Portal. Now, click New and then click on Data Services | Recovery Services | Recovery Site Vault | Quick Create. You'll need to enter a name for the vault you're creating, and you must specify the region in which the vault is to be created, as shown in **Figure 1**. Click Create Vault to complete the process.

Now that you've created the vault, it must be configured. Click on the Recovery Services tab and then click on the vault you just created. The first thing you'll need to specify is whether site recovery will occur between a Hyper-V site and Azure, or between two on-premises Hyper-V sites (see **Figure 2**).

Next, click on the Manage Certificates link. When prompted, provide the certificate (the .CER file) that you created earlier. Once the certificate has been uploaded, click on the Get the Vault Key link. Be sure to make a note of the key.

Azure Site Recovery Provider

When you run the executable file, Windows will display the Microsoft Azure Site Recovery Provider Setup wizard.

Now it's time to download the Azure Site Recovery Provider and install it on your Virtual Machine Manager servers. Select the Download Microsoft Azure Site Recovery Provider and Install it on the Virtual Machine Manager servers link. When prompted, save the file to a centrally accessible location. Now, shut down the Virtual Machine Manager service and then run the executable file on each of your Virtual Machine Manager servers.

When you run the executable file, Windows will display the Microsoft Azure Site Recovery Provider Setup wizard. Click Install to begin the installation process.

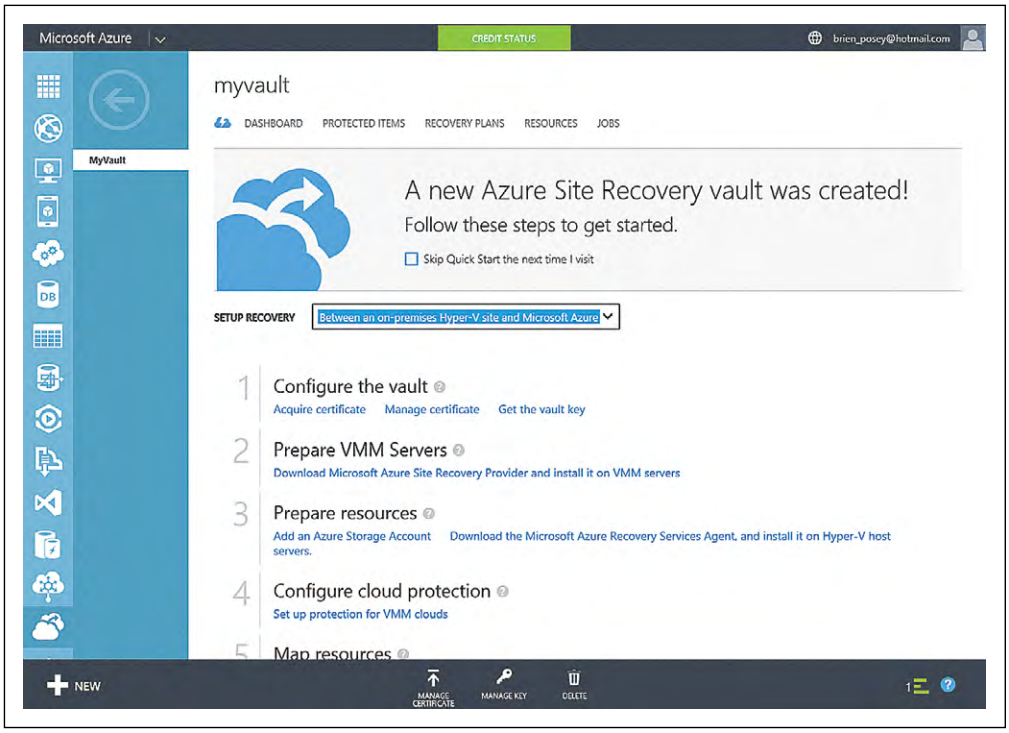


Figure 2. *Specifying the type of site recovery.*

You must specify your certificate, vault and key.

Figure 3. *You must specify your certificate, vault and vault key.*

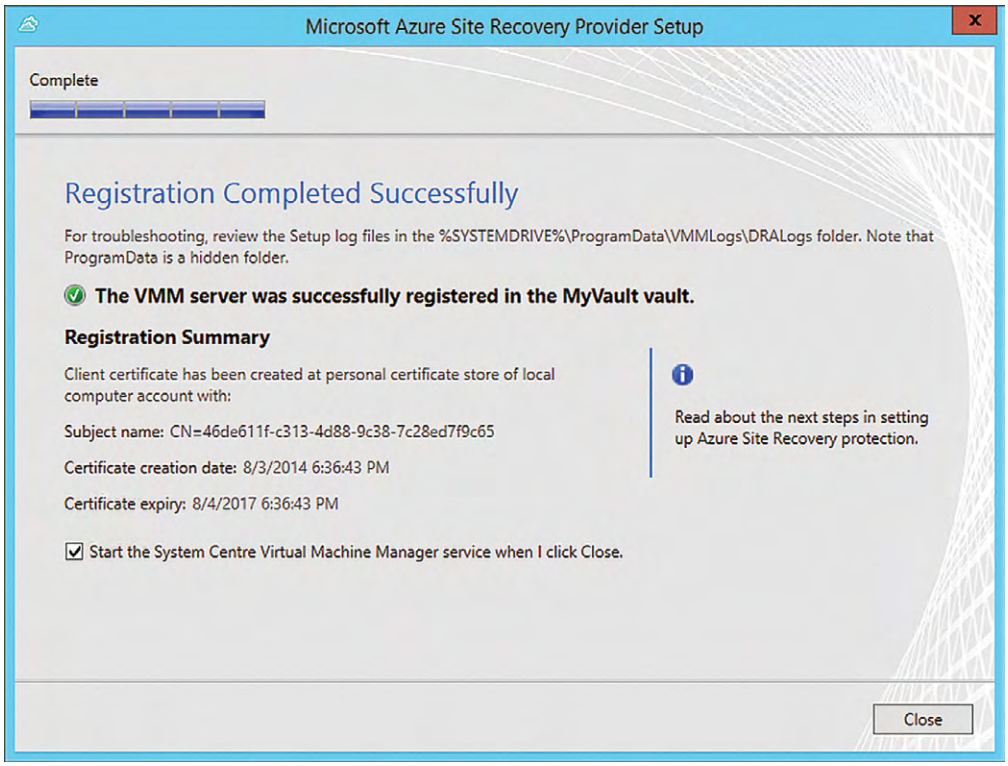


Figure 4. *Confirmation of a successful registration.*

After a few seconds, you should see a message telling you that Setup completed successfully. Click Next and you'll be prompted for your Internet connection settings. Click Next again and you'll be taken to the Vault Registration screen. You'll need to select your certificate and then specify your vault and your vault key (see **Figure 3**, p. 30).

Click Next and you'll see a prompt asking you if you want to encrypt replicated data. If you allow this option, an encryption certificate will be automatically generated. You'll have to provide this certificate whenever you fail over VMs. Click Next, followed by Register to complete the process. When the process completes, you should see a message confirming you've successfully registered the Virtual Machine Manager server with your vault (see **Figure 4**, p. 30).

To protect a private cloud, you must right-click on the private cloud within the Virtual Machine Manager console.

Protecting a Cloud

At this point, you've created a vault on Azure and associated the vault with Virtual Machine Manager. Usually, the next step in the process is to protect a private cloud. This will vary depending on your goals and whether you're replicating to Azure Storage or to a private cloud.

To protect a private cloud, you must right-click on the private cloud within the Virtual Machine Manager console (assuming the cloud isn't already being synchronized) and select the Properties command from the shortcut menu. When the cloud's properties sheet appears, go to the General tab and select the Send Configuration Data About this Cloud to the Azure Hyper-V Recovery Manager checkbox, and click OK. After doing so, go into Azure, click on your vault, and select the Protected Items tab. You should see your cloud listed in the vault, as shown in **Figure 5**, p. 32.

Click on the cloud and select the Configure Protection Settings link. You can now complete the process by answering questions about the protection you want. For instance, you're initially asked to select a target. This is where you would specify whether you want to replicate the cloud to Virtual Machine Manager or to Azure. After making this selection, you can specify your storage account (if you're synchronizing to Azure), as well as your copy frequency, recovery point retention period, and the frequency of application consistent snapshots (see **Figure 6**, p. 32). Click Save to save your changes.

Replicating a Virtual Machine Manager to the Microsoft cloud using Azure Site Recovery is a fairly straightforward process.

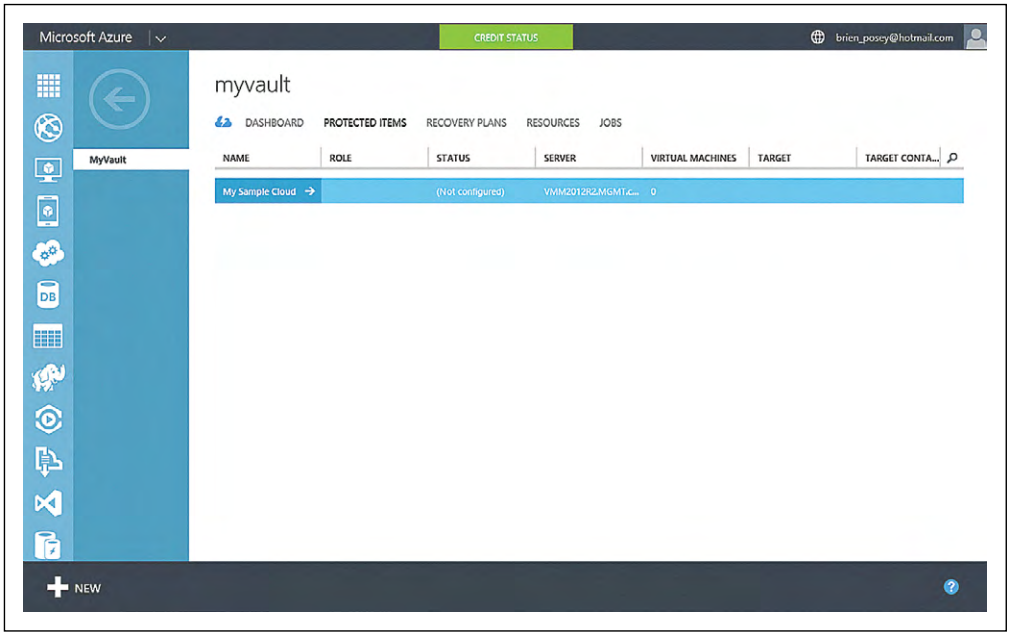


Figure 5. *The private cloud now appears in the vault.*

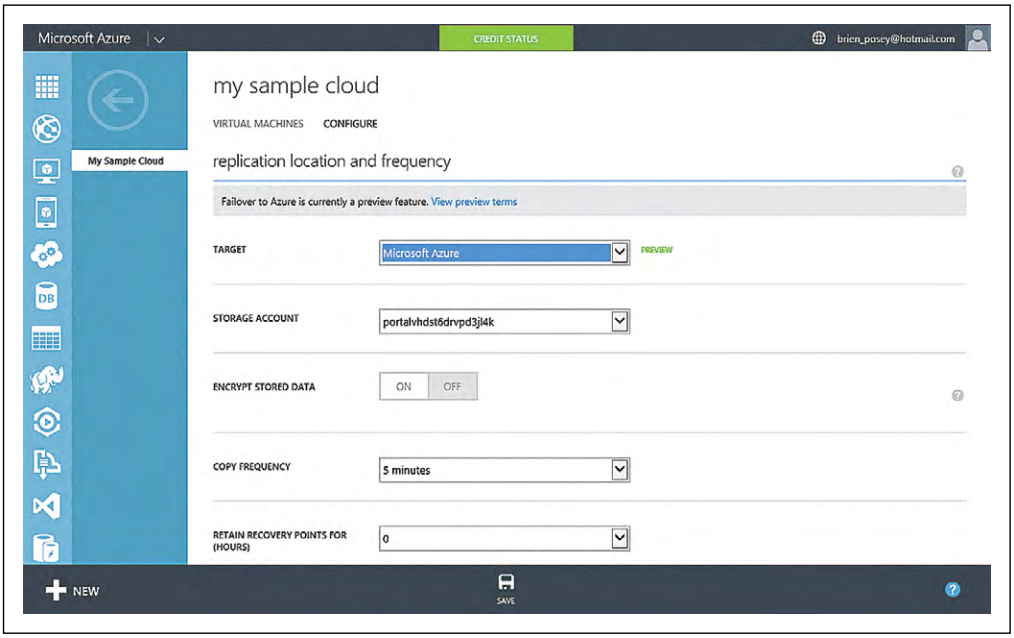


Figure 6. *Configuring the replication parameters.*

And that's it! Replicating a Virtual Machine Manager to the Microsoft cloud using Azure Site Recovery is a fairly straightforward process. The key to making the process work is to generate the certificates correctly. R

Brien M. Posey is a seven-time Microsoft MVP with more than two decades of IT experience. He's written thousands of articles and several dozen books on a wide variety of IT topics. Visit his Web site at brienposey.com.