Zerto

BEST PRACTICES WHEN PROTECTING VIRTUAL MACHINES RUNNING MSCS

ZVR-MSCS-4.0U6-01-14-01-16

This document is intended to cover best practices when using a Microsoft Cluster Server (MSCS). All information is correct for Zerto Virtual Replication version 3 and higher.

Zerto Virtual Replication is able to protect virtual machines that utilize Raw Device Mappings (RDMs). It is also possible to replicate from RDMs to preprovisioned RDMs of the same size in the recovery site.

Note: Zerto Virtual Replication for Hyper-V does not support Pass-through disks.

Supported Configurations

Support by Zerto Virtual Replication for virtual machines running MSCS is limited to enterprises only. Cloud service providers offering DR-as-a-Service (DRaaS) or In-Cloud DR (ICDR) cannot offer to protect virtual machines running MSCS using Zerto Virtual Replication.

Zerto Virtual Replication can protect virtual machines running MSCS in enterprises if:

- The virtual machines run Windows Server 2008 and higher.
- The Microsoft SQL Server database is Microsoft SQL Server 2005 and higher.
- The cluster is an Active/Passive cluster and a maximum 2 node cluster. Only the primary active preferred node is protected by Zerto Virtual Replication, replicating to a preprovisioned RDM in the recovery site. The secondary node is not protected by Zerto Virtual Replication. Thus, Zerto Virtual Replication cannot protect:
  - An Active/Active cluster.
  - An Active/Passive cluster with both nodes in the cluster configured to be protected.
- All of the Cluster services are configured to be dependent on each other to ensure they all exist on the same node at all times. If cluster services are on different nodes simultaneously, then one of them will always be in an inconsistent state.
- The recovery must be to a vCenter Server. VMware vCloud Director does not support RDMs and thus cannot be used as the recovery site for Zerto Virtual Replication VPGs protecting virtual machines running RDM-based MSCS.

Zerto Virtual Replication cannot protect virtual machines when:

- Target disks are VMDKs of the MSCS disk.
- The virtual machines are recovered to the same target RDM.
- VMDKs are used as shared cluster disks.
- iSCSI in-guest initiators are used to access shared cluster disks.

How Zerto Virtual Replication Works with MSCS

When protecting MSCS virtual machines with Zerto Virtual Replication the assumption is that the vast majority of writes to disk are from the primary node, so that the database and MSCS remain consistent. For this reason, only the Primary Active Node in an Active/Passive Cluster can be protected by Zerto Virtual Replication.

If the MSCS Active Node role is switched to the secondary node, which is not protected by Zerto Virtual Replication, during the period when the secondary node is the active node, any changes made to the RDMs are not replicated. Once the Active Node role is moved back to the primary node, the data on the recovery site will be in an inconsistent state, since the target RDMs in the recovery site are not synchronized with the protected RDMs that include the writes from the secondary node. To ensure that recovery using Zerto Virtual Replication is possible, you must synchronize the VPG that includes the primary node. Synchronizing the MSCS VPG returns the cluster to a protected and consistent state. This operation performs a delta sync, which scans both the source and target RDMs, then replicates any changes and inconsistencies found.

Forcibly Synchronize the VPG from the Zerto User Interface

You can forcibly synchronize the VPG in the Zerto User Interface after MSCS maintenance is completed, when the MSCS Active Node role is changed back to the node protected by Zerto Virtual Replication.

To forcibly synchronize a VPG using the Zerto User Interface:

1. In the Zerto User Interface, select the *VPGs* or *VMs* tab and click the VPG to display the VPG details.
2. In the dynamic tab that opens, click *MORE* > *Force Sync*.

   The VPG on the protected site is synchronized with the recovery site.

As the journal fills up during the synchronization process, older checkpoints are deleted from the journal to make room for new data, and the data prior to these checkpoints are promoted to the virtual machine virtual disks. Thus, during synchronization, you can recover the virtual machine to any checkpoint still in the journal, but as times passes the list of available checkpoints may be reduced, possibly removing the ability to recover. Therefore, Zerto recommends only performing this operation out of working hours if the journal still contains consistent checkpoints that are required.

Forcibly Synchronize the VPG Using Cmdlets

You can synchronize the protected virtual machines in the VPG using a Zerto Virtual Replication cmdlet.

Zerto recommends running a script on both primary and secondary nodes every minute. The script should check that the primary node is the active node and run the `Force-Sync` cmdlet automatically if the secondary node becomes the active node. The script should be run after the primary node returns to being the active node.

To forcibly synchronize a VPG by running the cmdlet:

Run the `Force-Sync` cmdlet.

```
Force-Sync [-ZVMIP] <String> [-ZVMPort] <Int32> [-Username] <String> [-Password] <String>
[-VirtualProtectionGroup] <String> [-Wait <int32>] [<Common&RiskParameters>]
```

The cmdlet is run from the PowerShell prompt as follows.

```
PS C:\Windows\SysWOW64\WindowsPowerShell\v1.0> Force-Sync
```

You are prompted for the name of the VPG to synchronize. The VPG name is case-sensitive. You are then prompted for the IP address of one of the Zerto Virtual Manager sites, either where the virtual machines in the VPG are protected or recovered, for the HTTP port used for inbound communication with that Zerto Virtual Manager, and a valid username and password, defined in the `users.txt` file for the Zerto Virtual Manager where the cmdlet is run, as described in *Zerto Virtual Replication PowerShell Cmdlets Guide*.

After the `Force-Sync` cmdlet completes, returning the command task identifier and site identifier, some time might still be needed before the VPG is fully resynchronized.

Additionally, the script can pause VPG protection if the RDMs are in an inconsistent state, using the `Pause-ProtectionGroup` and `Resume-ProtectionGroup` cmdlets. The script pauses the VPG if the nodes are in an inconsistent state so that it is clear that the VPG can no longer be failed over until synchronized.

To pause the protection of a VPG:

Run the `Pause-ProtectionGroup` cmdlet.

```
Pause-ProtectionGroup [-ZVMIP] <String> [-ZVMPort] <Int32> [-Username] <String>
[-Password] <String> [-VirtualProtectionGroup] <String> [-Wait <int32>]
[<Common&RiskParameters>]
```

The cmdlet is run from the PowerShell prompt as follows.

```
PS C:\Windows\SysWOW64\WindowsPowerShell\v1.0> Pause-ProtectionGroup
```

You are prompted for the name of the VPG to pause. The VPG name is case-sensitive. You are then prompted for the IP address of one of the Zerto Virtual Manager sites, either where the virtual machines in the VPG are protected or recovered, for the HTTP port used for inbound communication with that Zerto Virtual Manager, and a valid username and password, defined

in the `users.txt` file for the Zerto Virtual Manager where the cmdlet is run, as described in *Zerto Virtual Replication PowerShell Cmdlets Guide*.

Note: Zerto recommends adding a checkpoint to the VPG that you plan to pause, if you might want to recover the VPG to the latest point in time before it is paused. For details, see *Zerto Virtual Replication PowerShell Cmdlets Guide*.

To resume the protection of a VPG:

Run the `Resume-ProtectionGroup` cmdlet.

```
Resume-ProtectionGroup [-ZVMIP] <String> [-ZVMPort] <Int32> [-Username] <String>
[-Password] <String> [-VirtualProtectionGroup] <String> [-Wait <int32>]
[<Common&RiskParameters>]
```

The cmdlet is run from the PowerShell prompt as follows.

```
PS C:\Windows\SysWOW64\WindowsPowerShell\v1.0> Resume-ProtectionGroup
```

You are prompted for the name of the VPG to resume protecting. The VPG name is case-sensitive. You are then prompted for the IP address of one of the Zerto Virtual Manager sites, either where the virtual machines in the VPG are protected or recovered, for the HTTP port used for inbound communication with that Zerto Virtual Manager, and a valid username and password, defined in the `users.txt` file for the Zerto Virtual Manager where the cmdlet is run, as described in *Zerto Virtual Replication PowerShell Cmdlets Guide*.

Changing IP Addresses

Even though Zerto has the ability to automatically change the IP address of Windows virtual machines as part of a failover, move, or failover test operation, this feature should not be used if an MSCS cluster requires a new IP address in the recovery site. Therefore, Zerto recommends that, for an MSCS cluster, you preconfigure listeners on both the protected and recovery IP ranges, each node with a dedicated heartbeat NIC, so that only a simple DNS update to the new listener IP is required as part of a failover operation. If IP changes are required, this can easily be tested as part of a failover test operation as described below.

Failover Testing

To successfully perform a non-disruptive failover test of an MSCS virtual machine, Active Directory and DNS services are required to be online in the failover test isolated network. Therefore, Zerto recommends protecting an Active Directory Domain Controller, configured as the primary or secondary DNS server for the SQL Server virtual machine. Zerto Virtual Replication is used to bring an up-to-date copy of Active Directory online with ease for Failover Testing.

The Active Directory virtual machine should never be recovered to previous points in time in production and individual virtual machines cannot be failed over in a VPG. Therefore, Zerto recommends placing the Active Directory virtual machine in its own VPG and assigning both failover and failover test Network Adapters in the virtual machine to connect to an isolated test network.

Note: When booting Active Directory in an isolated test network, a minimum five minute window is required for Active Directory services to come fully online to allow MSCS services to start.