Association for Information Systems
AIS Electronic Library (AISeL)

SAIS 2022 Proceedings | Southern (SAIS)

4-1-2022

Disaster Recovery Management with PowerShell PSDRM

Steven Zavala
Sam Houston State University, Saz005@SHSU.EDU

Narasimha Shashidhar
Sam Houston State University, nks001@shsu.edu

Cihan Varol
Sam Houston State University, cxv007@shsu.edu

Bing Zhou
Sam Houston State University, Bxz003@SHSU.EDU

Follow this and additional works at: https://aisel.aisnet.org/sais2022

Recommended Citation

Zavala, Steven; Shashidhar, Narasimha; Varol, Cihan; and Zhou, Bing, "Disaster Recovery Management with PowerShell PSDRM" (2022). *SAIS 2022 Proceedings*. 23.
https://aisel.aisnet.org/sais2022/23

This material is brought to you by the Southern (SAIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in SAIS 2022 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

Disaster Recovery Management with PowerShell PSDR$_M$

Steven Zavala
Sam Houston State University
Saz005@SHSU.EDU

Narasimha Shashidhar
Sam Houston State University
Nks001@SHSU.EDU

Cihan Varol
Sam Houston State University
Cxv007@SHSU.EDU

Bing Zhou
Sam Houston State University
Bxz003@SHSU.EDU

ABSTRACT

Securing information and infrastructure is at the top of every organization's priority. Security solutions are necessary and when properly implemented can minimize the exposure of an organization's risk to compromise. Implementation can be costly and standardization is challenging. There are many cybersecurity solutions available ranging from open source to premium level coverages that can include deployment, monitoring, detection, and response. As threats evolve, the impacts of exploits become more difficult to thwart and in cases of ransomware the affects can immobilize a company and lead to lasting economic reprisal. Disaster Recovery provides an aspect of Cybersecurity and the most fundamental requirement for an organization to maintain continuity. When an organization publicly acknowledges compromise of their infrastructure regardless of the nature of the attack, the outfall is loss of confidence which inevitably impacts both internal and external stakeholders. This in turn leads to further efficiency loss to the businesses profitability as the primary resources are allocated to investigative and resolution matters. What this research's primary goal is to focus on Disaster Recovery and provide an executable with PowerShell at the backend to perform a selective approach to automating Disaster Recovery within Virtualization infrastructures. This research shows methods on which an administrator could build their project using native tools such as PowerShell, to provide their own customized automated Disaster Recovery solutions designed for Virtualized environments by initiating a backup, test, restore and conserve volatile state. Too often does an organization lack the necessary skillsets needed to bring an organization back to service after an attack as much has seen in the effect of Ransomware attacks. Providing these means for organizations gives those with less than a financial advantage a fighting chance against unanticipated attacks. We accomplish this by standardizing a method for the roles responsible in the organization for ensuring security measures are maintained using PowerShell.

Keywords

PowerShell Functions, IExpress, Disaster Recovery, Virtualization, Ransomware, PowerCli, Cmdlets.

AN AUTOMATED RESPONSE REDUCES THE NEED FOR HASTY CYBERSECURITY SOLUTIONS

Attacks come in many forms and one of these service-disrupting attacks such as ransomware has such a devastating impact on a business that can effectively cause them to be down for several days. Cybersecurity is so important that companies invest more towards that aspect according to [1] Cisco Security report in 2019 that 43% of mid-market organizations are spending $250,000 to $999,000 annually and as that trend continues to climb. For our research we provide a menu-based customizable executable that works with native commands within a virtualized environment. Often those responsible for making a financial decision have an abstract view of what cybersecurity solutions provide, tend to make hasty decisions on a product that makes guarantees without a full understanding of how the execution process occurs. In the case of ransomware attacks, organizations may decide to pay and receive the decryption keys but, this still leaves uncertainty about whether they are secure afterward or in the case of a logic bomb were to trigger another attack. The other hidden loss is that to integrity and the loss of confidence from stakeholders and investors which can lead to further costly litigations. According to Acronis, [2] 71 percent of companies targeted by ransomware attacks resulted in infected systems, and out of those successful attacks at least 20 percent of those computers become infected within the company.

LOGICAL REASONING FOR ON-PREMISE SOLUTION VS CLOUD DISASTER RECOVERY

Several factors can lead enterprises into utilizing an on-premise solution one of which is privacy concerns due to illicit captures also data persistence on the cloud would allow the probability of exposure during a breach and the eventuality of unauthorized access through the exploit of weaknesses in one's system. The other issue surrounding Cloud-based solutions for disaster

recovery is long latency issues and in a speed data-centric business model, the slow response would be devastating and costly. Designing an on-premise disaster recovery eliminates the long latency issues seen with Cloud-based solutions which are important for an industry that relies on real-time data to make important business decisions. Reliable connectivity is another factor when deciding on how effectively an organization employs disaster recovery solutions. A more recent example of such a breach involves the colonial pipeline shutdown. The economic impact of their impact as noted in ACM SIGSOFT Software Engineering Newsletter [3], such an attack, in this case, initiated an emergency declaration in 17 states for the United States.

OTHER WORKS USING POWERSHELL FOR DISASTER RECOVERY

Other research is done in this area left off with Disaster Recovery with Hyper-V replica and PowerShell [4] which at the time of its delivery in 2014 was sufficient to provide a Disaster Recovery method for smaller businesses and does not scale for larger industries. In the research done on Hyper-V replica, the fundamentals were covered by enabling Hyper-V replication and using existing cmdlets to configure, monitor, and test failover and hinted at task scheduling as a potential but, failed to progress with this further. According to Spiceworks, [5] VMWare is leading the field for enterprises at 79 percent than their runner-up Microsoft Hyper-V at 48 percent leaving quite a disparity between enterprise usage. There are alternate plugins for PowerShell cmdlets to perform functions of replications on various platforms with the use of [6] PowerCli.

PSDR$_M$ IS AN AUTOMATED AND ROBUST DISASTER RECOVERY SOLUTION

Too often we encounter limitations for a standardized approach and a great example is industrial applications do not always allow cloud-based solutions for recovery methods because too much risk involved with open connectivity to the outside world. In those cases, an on-premise solution would be a likely choice. Giving companies the tools to ensure business continuity is a game-changer for all industries because it levels the playing field for recovery methods against an attack that cripples a company. This research provides a standardized approach to maintaining business continuity by providing the automated restorative procedure within PSDR$_M$.

OVERVIEW DISASTER RECOVERY SOLUTION POWERSHELL METHOD

The custom program design to produce a standardized approach to disaster recovery is "PowerShell Disaster Recovery Management" (PSDRM), using PowerShell as a back-end method for performing Disaster Recovery steps such as creating a clone copy of a system shutting it down and deploying it to an isolated network to segment the system to prevent conflicting IP conflicts. The next piece highlights a front-end executable system that [7] Read-Host Switch input parameter, used for invoking a read line of input which prompts the user for an entry attached with a switch parameter for menu-like commands. The switch data then has combinations of actions that perform cloning a system, migrating between host from a VCenter managed server, performing a shutdown of VM, creating a snapshot, disconnecting network drives, and these actions mirrored for a Hyper-V infrastructure. The final piece is the executable that performs different scenarios from a menu item for example Snapshot Function, Clone Function, Migrate VM, Power On, Power Off, and Clean Up. The objective of these actions provides a method of cloning a machine to a sideloaded Host dedicated to storing running machines on a segmented network. The infrastructure runs a three Host system, and two are for Host redundancy for migration and provides continuity during maintenance and the third Host is reserved for disaster recovery provided an attack occurs such as ransomware, then what has occurred is a sideloaded hot spare outside of the scenarios then used for cloning and testing of a valid running VM. The executable includes a selection for what type of system so that it associates the right commands for the associated system giving the user an all-in-one box solution for different virtualized systems as in VMWare or Hyper-V. Different scenarios are required to forensic evidence when an attack has occurred so creating a snapshot to save the machine's volatile state is crucial for investigative measures so the machine can be shut down and cloned for deployment to the third host reserved for restoring cloned machines in a network isolated environment with a restorable snapshot. A menu item to perform these combination actions are used for simple iteration from non-technical users such as "ANOMALY – SNAPSHOT_ISOLATE" which performs a combination of the functions associated with capturing the machine's volatile state and deploying on an isolated network.

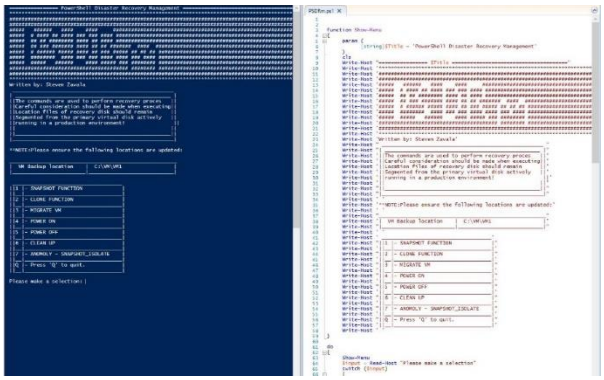

Fig. 1 Menu selection PowerShell Disaster Recovery Management

POWERSHELL ON-PREMISE DESIGN FOR PSDR$_M$

For an organization to maintain its competitive advantage over competing industries is to have a manageable process that is not only robust in its security posture but, has capable support staff to ensure and impose those security measures. In the next selection, we outline the process of enforcing a disaster recovery response application that will procedurally implement a recovery response that will ease the administrator's response to such an event. Through the standardization of such tools makes it financial feasibility into one's ability to maintain a robust security posture.

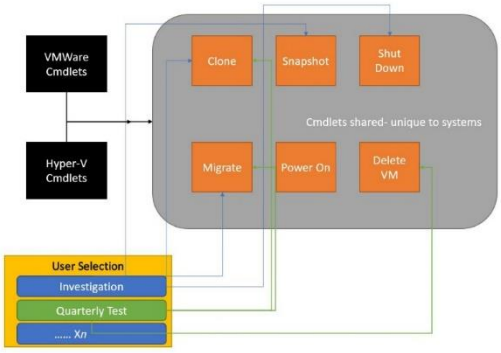

Fig. 2 Design User Interface Cross-Platform

Design Tool for your PowerShell Executable

PowerShell execution is achievable by the process of using a self-extracting executable otherwise an INF-based setup executable, or a compressed cabinet file, or via front-end interface. The application used to deploy this method of executing a self-extracting executable is by using [8] IExpress. This method allows the end-user to self-define their execution process based on their company's policy. The package self-extracting tool invokes the PowerShell ".ps1" file to run in an elevated privilege execution process. In Fig. 3 below we outline the execution process, in item one we show the prompt notification on startup of the executable, in item two we identify the license agreement for use of executable, and lastly, in item three we identify the call instruction to invoke the PowerShell executable this is the user interface that outlines the menu options for creating a snapshot, cloning a VM, Migrating, Power on, Power off, clean up, and Anomaly detection in which we discuss further in the next section.

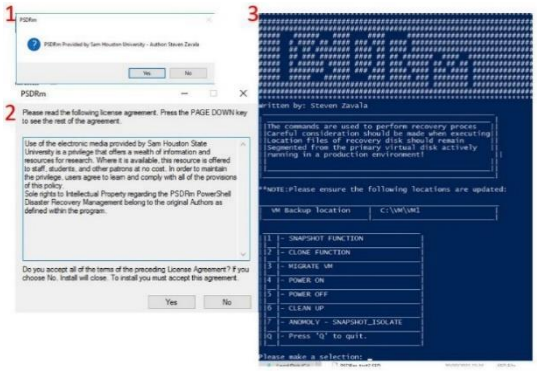

Fig. 3 IExpress Final Process "PSDRM" Executable

Menu Selection PSDRM

For an organization to maintain its competitive advantage over competing industries is to have a manageable process that is not only robust in its security posture but, has capable support staff to ensure and impose those security measures. In the next selection, we outline the process of enforcing a disaster recovery response application that will procedurally implement a recovery response that will ease the administrator's response to such an event. Through the standardization of such tools makes it financial feasibility into one's ability to maintain a robust security posture.

In the snapshot function, the purpose of PSDRM is to create a volatile state collection in the case of an initiating event through either a breach or active attacks, thereby triggering an investigative measure to mitigate the loss of the volatile state. Leaving this open to interpretation on response methods can be an unacceptable practice in today's environment as mentioned in a presentation from [10] SEI Software Engineering Institute at Carnegie Mellon University. Breadcrumbs leading back to the intent of the actions of the attacker is vital in capturing the machine's volatile state thus is a primary function in capturing this state and why this step is critical in the menu functions for PSDRM. For the section of PowerShell Create Snapshot menu, we utilize the snapshot management component to ensure that we preserve the state in the event of a breach and further analysis ensues. To create a snapshot, one will need to call the VM and pipe the command into the new create VM snapshot and define the name of the snapshot. We map this command "get-vm node | New-snapshot -Name nodename -description node description" to the Snapshot function menu. This will be used in the collective option to respond to an anomaly.

In the clone function, the purpose of PSDRM is to create a shadow environment to mimic the production environment and deploy a virtual machine as a [11] linked clone. The clone function intends to prepare a copy or replica of the existing node and send it to an alternate host assignment with shared resources and network resources via VLAN and promiscuous mode operation to allow specific communication. This function serves two purposes, one of which is for isolating a compromised machine onto a non-production machine and secondly allows for an alternate means of debugging and forensics evidence gathering. In the PowerCLI cmdlets, we utilize the snapshot management component to ensure that we preserve the state in the event of a breach and further analysis ensues. To create a snapshot, one will need to call the VM and pipe the command into the new create VM via the "Export-VM -Name node -path $location" to create a cloned image of the VM in an investigation. This portion will be mapped to the Clone Function.

In the migrate VM function, the purpose of PSDRM is to move the VM and the resources associated to an alternate environment. The migration is optionally performed as a [12] hot or cold state migration meaning that a node is moved in the powered-on stat or the powered-off state. The preference, in this case, is cold migration and the justification is utilizing the segmented network model to move the machine to an alternate Host for the intent of forensic analysis. In this step, it is important to segment a suspected node and the action is to migrate this to a VLAN segmented forensic management NIC in the event of a breach or compromise then segmenting an affected device would be crucial in securing one's environment. What we utilize in this instance is the command "Move-vm -vm node -Destination Host1", mapped to the migrate function. This will be used in the collective option to respond to an anomaly and it cast as the main importance of moving this system to a segmented network as defined by the organizational design.

The power on and off-state is crucial in selecting the right option. Too often are the differences in shutting down versus a shutdown operation misunderstood. The logic for adding this control is to eliminate the choices and only provide power on and power off options that functionally perform the [13] soft option for initiating the shutdown or startup method. The hard option is reserved for the last resort method and is the equivalent of pressing the shutdown key as opposed to allowing the machine to close out its operating system properly. The power on and off is used to place a system in a state that is ready to be moved to

another system and resume its operation to a running state afterward. In this operation, we utilize the command that is "Stop-VM -vm node" to power down the related node and places it into a state that would be ready to migrate to a segmented network. This will effectively be mapped to the Power off function. In the next operator we use the "Start-VM -vm node -confirm -RunAsync" to power on the node associated which starts asynchronously. This is effectively mapped to the Power on function.

In the clean-up state, the Virtual Machines are cleaned up of snapshots and deleted. This is reserved logically for post-incident response and forensic investigation closeout. In the post-investigation phase assuming the digital forensic analysis is complete and a resolution is deployed then the resources made to create a shadow copy of the affected environment are released. The action associate [14] deletes the machine from the disk permanently. In this selection, we use the command "Remove-Snapshot -Snapshot nodename -RemoveChildren" which completes the action of removing the snapshot associated with the node and its associated children. This is effectively be mapped to the cleanup function.

In the anomaly snapshot isolate selection, we employ the collective actions of capturing a snapshot powering down the machine, migrating it to the alternate host, restoring the snapshot, and powering on the virtual machine. A response scenario left to respondents leaves room for error. Using this method allows for one execution process that meets most standard governance policies but, allows the user to build their design based on what fits their security model and response actions to breaches and attacks.

PSDR$_M$ TOOL EVALUATION CLOUD DATA RECOVERY VERSUS ON-PREMISE DATA RECOVERY

The PSDRM provides a scalable solution for both on-premise and cloud solutions and optimized for an on-premise solution. A comparison on value scorecards is provided to show factors based on assumptions of business needs on acceptable Recovery Rime Objectives (RTO) shared in [16] Harbinger's statement on the importance of data backup and recovery. In the following assessment, the assumption of valuation is made based on the critical nature of production environments in the case of Industrial Control Systems which primarily utilize an on-premise solution. Cloud solutions for Industrial Control Systems are consistently being challenged as a viable solution for manufacturing solutions and have been echoed in various attempts to introduce the internet of things into a process control environment or [17] Cloud operating systems for industrial applications. One of the biggest challenges is the latency one encounters from Cloud environments. Each column factor is based on a scale rating of 10 for the categories of Ease of implementation, overall simplicity, cost, management consistency, and scalability. In the category of time and application compatibility we use a higher scale rating of 40 due to a higher variability on value assessment. $(\frac{a}{n^1} + \frac{b}{n^2} + \frac{c}{n^3} + \cdots \frac{n}{n^n}) \; / \; \Sigma$

Factor	Ease of getting Started 1-10 rating	Simplicity 1-10 rating	Time 0-40	Cost 0-10	Management Consistency 0-10	Scalability 0-10	Response Time and Latency 0-40	Application Compatibility 0-40	Total Value Assessment (%)
Cloud Data Recovery	One just needs to configure services provided by cloud provider	Simplified environment, reduced complexity of recovery. Improved recovery reliability by maximizing features of automation and cloud technologies, thus minimizing risk of failure to recover	Significantly shortened server recovery time	As mentioned above, there is no need to purchase huge infrastructure to store their data. Cloud based data storage solutions enables small and midsize businesses to have the same RTO, RPO and security as any large organization, without having to deal with significant overheads.	Cloud providers simply have services setup which will take care of everything. You don't need to worry about day to day activities required to ensure data recovery objectives	Easily scalable as per your business needs	A CSP can store data in diverse locations far apart from each other according to his feasibility. This can give rise to latency issues. Cloud based storage solutions are not recommended for applications that demand high response times and low latency	With cloud based recovery service , one needs to ensure that their applications are compatible with the CSP's infrastructure. For example some applications may require a specific environment for them to run, which might not be available with the CSP	
Cloud Data Recovery Scorecard	9	8	35	8	9	9	35	20	
AVG	0.9	0.8	0.875	0.8	0.9	0.9	0.875	0.5	81.88%
Cloud Data Recovery Logic	Highest rating some configurations but, no guarantee it will be fast or slow	Scored high but, slightly less because owners don't have oversight which depending could make it complex to provide a complete solution	Scored high but, slightly low because it implies that there is still downtime	Cost improves is a great factor but, slightly less depending on the cost with competitive pricing vs services and brand	Highest scoring across a plus for reducing cost as resources for organizations	Highest value no need to worry about growth	This is scored midway due to depends on the business need but, this is not great overall but meets business need	This is scored midway due to depends on the business need but, this is not great overall	
Traditional On Premise Data Recovery	Deploying and Managing an on premise data recovery plan usually tends to be complex, requiring significant timeline, budgets and resources you might not have	Building an all-inclusive data recovery plan can be complex when compared to cloud based recovery, irrespective of whether you do it yourself or outsource it to a service provider	Recovery time can range from couple of days to weeks	A secondary data recovery site to enable redundancy can drive upwards your costs in a major way, for example you would need an additional space, more manpower to manage the center, power and cooling bills etc.	As the data recovery processes evolve continuously, one needs to upgrade to new skill set on an ongoing basis to ensure data recovery objective compliance	Does not scale up or down easily	Mostly an organizations physical data recovery site is located at the nearest feasible location to ensure high response times and thus reducing latency issues	For highly custom applications, one should opt for physical DR	
Traditional On Premise Data Recovery Scorecard	2	3	2	4	4	2	39	20	
AVG	0.2	0.3	0.05	0.4	0.4	0.2	0.975	0.75	40.94%
Traditional On Premise Data Recovery Logic	This is not great due to budgetary needs or resources availability it may consume a large amount of time	A lot of in house development	This may be too long for a business to be without services. Not great	Increased budgetary needs but, may be perceived as cost of doing business	Not great either for an organization that needs to be productive and strapped for resources may not be feasible	This not great as businesses can be dynamic in needs and need to scale based on consumer needs	This is the best option for reducing latency	Physical DR are an easier decision to make but will be an extra cost	
PowerShell Disaster Recovery Management PSRDm	Built in cmdlets no additional libraries needed	Complete built application with no needs to download additional packages just PowerShell cmdlets and Existing knowhow	Already built but, some time to customize and fairly easy to do. Recovery is actively available but limitation to resource availability	zero cost only time resource	PowerShell cmdlets continue to be supported across multiple platforms and will expand their compatibility	Does scale up for any need. Does require additional configuration	Onsite solution so low latency	Application fits need due to native commands and in house flexibility	
PowerShell Disaster Recovery Management PSRDm Scorecard	9	8	35	8	9	8	39	39	
AVG	0.9	0.8	0.875	0.8	0.9	0.8	0.975	0.975	87.81%
PowerShell Disaster Recovery Management PSRDm Logic	Lightweight no need for additional packages	Fairly easy with the type of functions built in to make all has style choices	Scored higher because DR plan adds running copy to environment and has an additional like for like replacement as the need arises.	This is by far the best only need to account for time as resource from in house users to customize	No issues with PowerShell becoming obsolete	Because of the native language as OS upgrade this will never be an issues as environments grow	Low latency same as on premise solution	scored high due to flexibility and native commands	

Factor	Ease of getting Started 1-10 rating	Simplicity 1-10 rating	Time 0-40	Cost 0-10	Management Consistency 0-10	Scalability 0-10	Response Time and Latency 0-40	Application Compatibility 0-40	Overall Value
	A	B	C	D	E	F	G	H	I
Cloud	0.9	0.8	0.875	0.8	0.9	0.9	0.875	0.5	0.8188
Trad On Prem	0.2	0.3	0.05	0.4	0.4	0.2	0.975	0.75	0.4094
PSDRm	0.9	0.8	0.875	0.8	0.9	0.8	0.975	0.975	0.8781

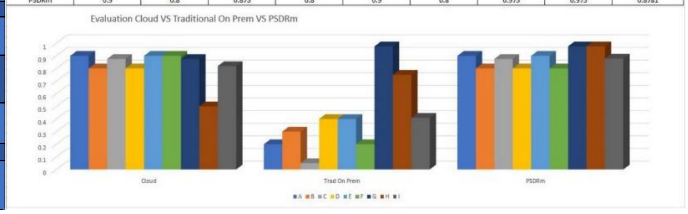

Fig. 4 Value Assessment PSDRM VS On-Prem VS Cloud Data Recovery Solutions

CONCLUSION

With as many breaches occurring at an ever-increasing frequency it foreshadows a story of a more emboldened attacker. The attackers are more organized and work as structured corporations rather than the perceived hooded hacker working alone. This dynamic of Cyber threats has taken a completely new shape that put the less financially stable companies at greater risk and stretches their business continuity to its absolute highest tension. Without leveling the playing field and eliminating some of

those concerns a company is doomed to fail. There are many avenues to breach prevention but, PSDRM is the best fighting chance against business continuity disruption.

REFERENCES

1. The Security Bottom Line Report, [Online]. Available: https://www.cisco.com/c/dam/en/us/products/se/2019/10/Collateral/security-bottom-line-cybersecurity.pdf [Accessed: 3 February, 2021].
2. Understanding the true, hidden costs of ransomware attacks on the business, James R. Slaby [Online]. Available: https://www.acronis.com/en-us/articles/costs-of-ransomware-attacks/ [Accessed: 5 February, 2021].
3. Risk to the Public, Peter G. Neumann [Online]. Available: https://dl.acm.org/doi/10.1145/3468744.3468746 [Accessed: 17 September, 2021].
4. G. Jayaseelan and P. J. Charles, "Automated Secured Disaster Recovery with Hyper-V Replica and PowerShell," 2014 World Congress on Computing and Communication Technologies, Trichirappalli, India, 2014, pp. 150-153, doi: 10.1109/WCCCT.2014.60.
5. The 2020 State of Virtualization Tecnology, [Online]. https://www.spiceworks.com/marketing/reports/state-of-virtualization/. [Accessed: 11 March, 2021].
6. Install PowerCLI, [Online]. Available: https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.esxi.install.doc/GUID-F02D0C2D-B226-4908-9E5C-2E783D41FE2D.html [Accessed: 11 March, 2021].
7. Read-Host, [Online].Available: https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.utility/read-host?view=powershell-7.1 [Accessed: 11 March, 2021].
8. IExpress Wizard for Windows Server 2008 R2 with SP1, [Online]. Available: https://docs.microsoft.com/en-us/internet-explorer/ie11-ieak/iexpress-wizard-for-win-server [Accessed: 09 August, 2021].
9. The Windows PowerShell ISE, [Online]. Available: https://docs.microsoft.com/en-us/powershell/scripting/windows-powershell/ise/introducing-the-windows-powershell-ise?view=powershell-7.1 [Accessed: 09 August, 2021].
10. Volatile Data Collection, [Online].Available: https://fedvte.usalearning.gov/courses/CSI/course/videos/pdf/CSI_D01_S05_T01_STEP.pdf [Accessed: 11 August, 2021].
11. Using Linked Clones, [Online]. Available: https://docs.vmware.com/en/VMware-Workstation-Pro/16.0/com.vmware.ws.using.doc/GUID-BA264A65-C50F-4345-A787-DCC5C5324DD1.html [Accessed: 11 August, 2021].
12. VMWare Docs, Migrating Virtual Machines, [Online]. Available: https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.vcenterhost.doc/GUID-FE2B516E-7366-4978-B75C-64BF0AC676EB.html [Accessed: 11 August, 2021].
13. VMWare Docs, Configure Power Options and Power Control Settings, [Online].Available: https://docs.vmware.com/en/VMware-Workstation-Pro/16.0/com.vmware.ws.using.doc/GUID-F3E4C12E-666A-4C92-AA74-B7B40C56F37C.html [Accessed: 11 August, 2021].
14. VMWare Docs, Delete a Virtual Machine, [Online]. Available: https://docs.vmware.com/en/VMware-Workstation-Player-for-Windows/16.0/com.vmware.player.win.using.doc/GUID-281A4E91-1B6F-4486-8696-EC04C7D5DC5B.html [Accessed: 11 August, 2021].
15. PowerCLI 12.4 User's guide, [Online]. Available: https://developer.vmware.com/docs/14541/powercli-12-4-user-s-guide/GUID-0CBA540A-1D6F-4AF8-B140-DC8561AA9696.html [Accessed: 11 August, 2021].
16. Harbinger Systems, Cloud Vs Traditional On Premise Data Recovery, [Online].Available: https://harbinger-systems.com/blog/2014/05/cloud-vs-traditional-on-premise-data-recovery/ [Accessed: 11 August, 2021].
17. G. Xiong, T. Ji, X. Zhang, F. Zhu, and W. Liu, "Cloud operating system for industrial application," 2015 IEEE International Conference on Service Operations And Logistics, And Informatics (SOLI), 2015, pp. 43-48, doi: 10.1109/SOLI.2015.7367408.