VA Enterprise Design Patterns
Information Technology (IT) Service Management

Disaster Recovery as a Service

Office of Technology Strategies (TS)
Office of Information and Technology (OI&T)

Version 1.0
Date Issued: April 2017

Approval Coordination

Gary E.
Marshall
137891

Digitally signed by Gary E. Marshall
137891
DN: dc=gov, dc=va, o=internal, ou=people,
0.9.2342.19200300.100.1.1=gary.marshall
@va.gov, cn=Gary E. Marshall 137891
Date: 2017.04.20 09:08:43 -04'00'

Gary Marshall
Director, Technology Strategies, ASD

Deeneen U
Akeo
622220

Digitally signed by Deeneen U
Akeo 622220
DN: dc=gov, dc=va, o=internal,
ou=people,
0.9.2342.19200300.100.1.1=deen
een.akeo@va.gov, cn=Deeneen U
Akeo 622220
Date: 2017.05.08 11:40:33 -04'00'

Paul A. Tibbits, M.D.
DCIO Architecture, Strategy, and Design

Revision History

Version	Date	Approver	Notes
1.0	10/7/2016	Jaqueline Meadows-Stokes	Final version for TS leadership approval and signature, including all applicable updates addressing stakeholder feedback and Section 508 Compliance

CONTENTS

QUICK JUMP

Select an icon to skip to a section.

Current Capabilities

Future Capabilities

Use Cases

One-VA Technical Reference Model

The Veteran-Focused Integration Process

Enterprise Design Pattern Scope

1 INTRODUCTION

A conventional approach to Disaster Recovery (DR) consists of a secondary physical site for failover, with capital expenditures (CapEx) in Information Technology (IT) systems and infrastructure, and operating expenditures (OpEx) in maintenance and personnel. Cloud-based DR utilizes virtual machines (VMs) to backup and restore the IT systems of a primary site, allowing organizations to pay only when synchronization, testing, or failover is necessary. Disaster Recovery as a Service (DRaaS) is an enterprise service provided by a third party that restores IT systems in a local environment, or a public/private cloud-based environment, in the event of a natural disaster, human error, or test. At the Department of Veterans Affairs (VA), DRaaS provides a cloud-based service that enhances Recovery Time Objective (RTO) and Recovery Point Objective (RPO), without requiring upfront infrastructure planning within data centers.

VA’s objectives for utilizing enterprise-wide DRaaS include:

- **Enhanced Performance**: Failover to the cloud improves recovery time for IT systems in the event of a disaster

- **Optimized Resources**: Service provider-managed DR shifts the staff allocation toward Disaster Recovery Plan (DRP) development. Refer to the DR Planning Enterprise Design Pattern (EDP) for more detailed information[1]
- **Cost Reductions**: The "pay per use," or subscription model, reduces hardware and infrastructure expenditures, making DRaaS a cost effective DR solution

1.1 Business Problem

One of the chief DR problems observed within VA is data failover. According to current industry standards, data failover is caused by a lack of uniformity in a data recovery solution that is innovative and formidable.

DRaaS is not fully utilized at an enterprise level at VA; this creates risks that include issues for recovered data reliability, inefficient use of hardware resources, and higher costs for data recovery following a natural disaster. Additional enterprise risks and shortfalls include:

- VA has not currently completed its approach to leverage DRaaS
- The Federal "Cloud First" strategy has not been achieved
- VA has not maximized the use of an externally managed DRaaS for DR

While some VA regions are using industry DR services, and VA is continuing to adopt a cloud-based approach, a comprehensive and standard DRaaS solution is not yet available.

1.2 Business Need

In August 2012, the VA Memorandum, "Server Virtualize First Policy," was published by the Office of Information and Technology (OI&T) as a foundational step toward the implementation of the Federal "Cloud First" strategy and VA Directive 6517. VA policies require virtual server hardware for IT systems, in order to significantly benefit the entire organization in the areas of cost effectiveness, high availability, resource efficiency, and flexible application recovery options.

To meet VA and Federal policy mandates, VA must include externally managed DRaaS as part of its IT service offerings. DRaaS can lower costs and use automated virtual platforms to minimize the recovery time that follows a disaster. Minimized recovery time increases VA's Primary Mission Essential Function (PMEF) support. The technologies that VA needs to incorporate for DRaaS will drive decisions on how to optimize people and processes associated with DR. DRaaS is needed across VA to:

[1] https://www.oit.va.gov/programs/techstrategies/edp.cfm

- Decrease upfront IT resource investment
- Create a comprehensive and robust replication for faster standup
- Enhance performance by providing a dynamic level of critical system protection
- Allow the availability of high risk-mitigated data
- Use hardware resources efficiently

1.3 Business Case

VA's use of DRaaS addresses challenges to restoring enterprise IT services rapidly, in response to potential disruptions or emergencies. DRaaS enhances utilization of more advanced testing opportunities, including failover and failback testing, thereby instilling confidence in VA DR processes and procedures. DRaaS also removes VA's need to purchase hardware and pay for the operation of a secondary location. DRaaS enables VA to:

- Take advantage of service provider advancements in platform technologies and services
- Reduce costs through the use of a service provider's environment
- Leverage secure network connections and data encryption that will help meet strategic requirements. (Refer to the Cloud Security EDP for information on Cloud Security)[2]
- Free up resources that can be used in other strategic IT areas
- Enhance VA's ability to comply with financial and healthcare regulations

The benefits of such an approach include:

- Provides specialized expertise and managed services that ensure reliable DR on a continuous basis
- Significantly reduces costs for DRaaS-based replication, failover, and recovery, as compared to traditional, in-house DR, and some managed services alternatives

1.4 Approach

This EDP defines a framework for using DRaaS solutions. It addresses the following:

- Criteria for selecting a DRaaS solution
- Support for new environments and legacy systems with DRaaS capabilities
- Challenges with DRaaS solutions

The DRaaS EDP approach consists of the following:

[2] https://www.oit.va.gov/programs/techstrategies/edp.cfm

- Best practices for utilizing DRaaS solutions that are consistent with policy and applicable industry standards, such as provided by the National Institute of Standards and Technology (NIST)
- Enterprise criteria for new and legacy systems that execute a DRaaS solution
- DRaaS solutions for mitigating risks

2 CURRENT CAPABILITIES AND LIMITATIONS

2.1 Current Capabilities

VA has a wide array of tools in place for DR for different information systems. There are some existing agreements with industry that provide a variety of DR services to VA; however, these DR solutions are not externally managed DRaaS solutions. Also, an enterprise utilization framework for DRaaS has not been established at VA. There is no current DR Toolset within VA that meets the standard for DRaaS, based upon best practices and industry advancements.

A physical DR solution refers to the use of physical devices, such as servers and data storage devices, to capture, preserve, and restore data at an alternate offsite location. There is a need for similar or identical hardware, which would need to be configured and updated in lockstep with each other. In some cases, this could be cost prohibitive. Examples of systems using physical DR solutions at VA include:

- Veterans Health Information Systems and Technology Architecture (VistA) production systems
- Exchange 2007 Solution

VA currently works to deliver the following DR services for those systems:

- Reconstitution
- Failover with offsite storage

A virtual DR solution uses VMs and other virtual infrastructure to represent DR in logical terms, eliminating the need for a physical replica of the environment. When compared with physical DR solutions, a virtual DR solution provides a more efficient approach to managing computing resources and data than a physical DR solution. VA utilizes virtual DR solutions for the complete recovery of systems across 188 VA hospitals (non-VistA VM environment, file systems and designated physical servers). This includes a combination of internal DR services at VA data centers, and external backup services with an industry partner.

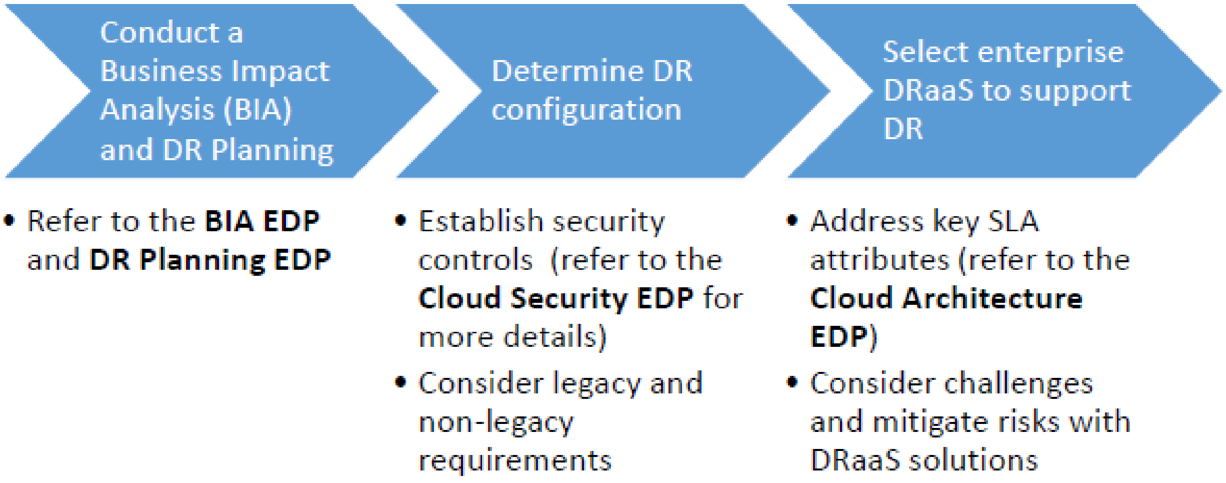
A cloud DR solution refers to a DR backup-and-restore strategy that involves storing and maintaining copies of electronic records in a cloud computing environment. Effective cloud DR provides continuity for services and the ability to failover to a second site at a lower than traditional DR cost, if there is a hardware or software failure of IT systems.

2.2 Current Limitations

At an enterprise level, VA does not currently subscribe to a managed service provider that has the potential to eliminate resourcing and associated costs; and provide the current industry expertise that is needed to effectively protect an enterprise in the case of a disaster. While there are instances of physical, virtual, or cloud DR across VA, none of these solutions provides the benefits or impact of using an enterprise level managed DRaaS solution to provide data protection and data integrity. A comprehensive and standard approach to DRaaS would eliminate potential gaps in data collection and retention that occurs when DR is implemented within organization silos.

3 Future Capabilities

A summary of the enterprise approach for DRaaS at VA can be found in Figure 1.



Conduct a Business Impact Analysis (BIA) and DR Planning

- Refer to the **BIA EDP** and **DR Planning EDP**

Determine DR configuration

- Establish security controls (refer to the **Cloud Security EDP** for more details)
- Consider legacy and non-legacy requirements

Select enterprise DRaaS to support DR

- Address key SLA attributes (refer to the **Cloud Architecture EDP**)
- Consider challenges and mitigate risks with DRaaS solutions

Figure 1: DRaaS Enterprise Approach

3.1 Criteria for Selecting a DRaaS Solution

To select an optimal DRaaS solution that will meet Enterprise DR needs, VA will evaluate a cloud management platform. This evaluation will document consistency across VA in its approach to standardize the use of DRaaS. VA will also conduct an internal DR assessment and follow an enterprise evaluation criterion for DRaaS.

3.1.1 Conduct an Internal DR Assessment

Prior to assessing external DRaaS solutions, VA will determine the following:

- The period of acceptable downtime and level of data loss; Key Performance Indicators (KPIs) include specific RPO/RTO objectives
- Prioritization of environments and systems based on mission criticality
- The need for an Active-Active configuration, which:
    - Maintains service availability, such that users will not notice any change in service if a momentary failure occurs
    - Eliminates the need for planned downtime as active users can be switched to the other node in the configuration
    - Provides risk-free failover testing in seconds, as opposed to minutes or even hour

Refer to the Business Impact Analysis (BIA) EDP and DR Planning EDP for more information on these topics.[3]

3.1.2 Evaluation Criteria for DRaaS Providers

VA will employ best practices for utilizing DRaaS solutions that are aligned with policy and industry standards. The key attributes that need to be evaluated when considering different DRaaS solutions are addressed in the Service Level Agreement (SLA), which must be developed and negotiated before selection. Several organizations have produced best practices on SLA structure and content.[4] Refer to the Cloud Architecture EDP for more detailed guidance on evaluating Cloud Service Provider (CSP) SLAs.[5]

The following are key attributes for recovery capabilities when selecting a DRaaS solution. VA will address these areas through a SLA, as summarized in Table 1 below.

[3] https://www.oit.va.gov/programs/techstrategies/edp.cfm

[4] MITRE Cloud SLA Considerations for the Government Consumer, July 2015

[5] https://www.oit.va.gov/programs/techstrategies/edp.cfm

TABLE 1: KEY DRAAS ATTRIBUTES AND SOLUTION FEATURES

Attribute	Key DRaaS Solution Feature
Security and Encryption	• Vendor Security Controls • Privacy Guarantees • Vendor Position Regarding Customer-Requested External Security Controls • Vulnerability and Consequence Assessment and Management • Risk and Issue Resolution • Data Ownership, Protection and Control
Monitoring and Control	• Incident Response and Reporting • DR and Service Failure Management • Outage Resolution • Continuity-Related Definitions • Access to VA data and applications in the providers environment
Recovery Capabilities	• Levels of Service Available • Performance Metrics • Quality Assurance, Performance Data Requirements • Measurement Methods • Service Level Improvement

Security and Encryption

There must be a clear understanding by VA on the willingness of the CSP to accommodate requested external security controls. VA should understand the methods by which the CSP intends to manage vulnerabilities, as well as the CSP's position regarding data ownership, protection, and control. The following should be specified to VA by the CSP:

- Information relating to the confidentiality and integrity of the services and the security controls which apply to the services
- How Privacy and Personally Identifiable Information (PII) will be handled in relation to the Cloud services
- Any disclaimers relating to security or critical processing, as wells as recommendations made by the CSP regarding independent backup of data stored in their Cloud, will be assessed
- How VA will push data to the CSP via encrypted channels (e.g., with keys that VA owns and configures)

In a DRaaS solution, it is important to understand the classification of the system or application that the DR solution will support, which are driven by Confidentiality, Integrity and Availability

(CIA). VA will consider that few CSPs currently meet the Federal Risk and Authorization Management Program (FedRAMP) High Baseline Requirements. Any immediate implementation of DRaaS that must support the High security baseline will be conducted through an externally managed private cloud (e.g., Terremark) or on-site private cloud at one of VA's IT Centers, until a DRaaS solution provided by external vendors receives a FedRAMP High Provisional Authority to Operate (P-ATO). As CSPs close the gap on meeting FedRAMP requirements, VA will migrate to a complete externally managed public cloud DRaaS solution. Refer to the Cloud Architecture EDP and Cloud Security EDP for more details on data classification.

Monitoring and Control

Key attributes that need to be addressed when verifying service capability, continuity, and outages by the CSP include, but are not limited to:

- Definition of a service outage
- Level of redundancy in place to minimize outages
- The need for scheduled downtime
- Frequency at which the CSP tests their own DR and Business Continuity Plan (BCP)

The following techniques must be provided in order to mitigate service failure:

- Multiple redundant data centers that are geographically available across multiple regions concurrently
- Replicated data stores
- Multiple redundant networks and other data center services, targeting a service level of concurrently maintainable services using divergent resources/paths
- Multiple app instances
- Automated failover

When services are not continuous, the burden of proof requires verification. The CSP should respond to the outages that are not caused by VA infrastructure. When burden of proof is a particular risk area, VA should carefully consider whether the SLA is sufficiently explicit in regard to roles and responsibilities, especially in events that interrupt continuous service.

Recovery Capabilities

VA will monitor and manage the DRaaS used. For each level of service offered, VA will ensure that effective service management and monitoring can be performed, including:

- Auditing
- Monitoring and reporting on a set of agreed to performance metrics
- Measurement & metering methods
- Service level improvement thresholds

Common features and corresponding options that should be available in the DRaaS solution are determined by the RTO and RPO needed, as listed in Table 2.

TABLE 2: RECOMMENDATION FOR COMMON DRAAS CAPABILITIES

DRaaS Feature	Options
DR Standby Operational Scenarios	• Cold Sites • Warm Sites • Hot Sites • Mirrored Sites
DR Recovery Types	• Simple backup solution with integrated offsite/cloud capabilities • Hybrid • Integrated/Orchestrated • Mission Critical
DR Architectures	• Backup and Restore • Pilot Light • Warm Standby • Multi-site
Data Storage	• Retention of data for a specific time period, ensuring the availability of an extended period of time in order to meet compliance requirements • Storage of multiple copies of data and the ability to do geographic redundancy in order to restore in more than one cloud region • Capability to define different sets of data associated with applications so that they can be individually failed over or prioritized
Compatibility	• Built in DR testing, as well as testing that does not compromise production systems • Support for existing storage replication technologies at VA • Support for existing Operating Systems (OSs) used at VA (Windows and Linux)
Functionality	• The option to transition from a Cold DR solution to a partially or fully automated Warm DR scenario • Replication and orchestration by handling multiple Hypervisors and physical systems

DRaaS Feature	Options
	• Open-standard Application Programming Interface (API) and scriptable interfaces so that automation can be specially tied into VA Cold DRaaS enhanced back-up capabilities

3.2 Supporting New Environments and Legacy Systems

VA will utilize an enterprise framework that identifies requirements for a DRaaS solution to support new and legacy systems within VA infrastructure. The framework outlines objectives for meeting VA data CIA requirements; and guarantees meeting VA RPO/RTO, while allowing reliable, predictable, and testable recovery in the cloud.

3.2.1 New Systems

For new or modern environments that consist of IT systems that are already cloud based, VA will need to consider:

- Network bandwidth and data transfer rates required to support data and application backup, recovery and reconstitution
- Network latency requirements of new systems for both end-user and system integration needs (e.g., colocation requirements of integrated back-end systems)
- Network bandwidth, latency, and data transfer rates required to support the fully loaded production system after a disaster event
- The system failover priority based on VA needs
- Flexible recovery options, such as restoring a single application or the whole infrastructure
- Availability and DR (RTO/RPO) business needs for the new systems

For new systems executing a DRaaS solution, a framework should consist of the following process:

- Establish the required availability and DR (RTO/RPO) requirements
- Determine the required data storage necessary for backup, restoration, and reconstitution of the system data and applications. This includes Workload Transfer parameters, which indicate how quickly static data and live workloads can be transferred; these have a direct impact upon how quickly VA can recover critical business processes
- Determine the Federal Information Processing Standard Publication (FIPS) 199 Federal Information Security Management Act (FISMA) data classification:

    - FISMA Low – limited adverse effect on VA operations, assets, or individuals if data is lost
    - FISMA Moderate – serious adverse effect on VA operations, assets, or individuals if data is lost
    - FISMA High – catastrophic adverse effect on VA operations, assets, or individuals if data is lost
- Determine the level of facilities required to support protection of the new system:
    - Cold Site – A DR service space where VA is responsible for providing and installing the necessary equipment needed to continue operations
    - Warm Site – Has allocated hardware, virtual infrastructure capacity, and configurations; and connectivity is already established and might have backups on hand, but they may not be complete and may be between several days and a week old, which would affect how quickly VA could be operational; might require system start-ups
    - Hot Site – A commercial DR service that maintains a running state for all equipment and virtual infrastructure needed for an enterprise continuation of computer and network operations, in the event of system or network failure
    - Mirrored Site – A site that provides continuous replication/mirroring of data sets between the data center and the cloud; and a "hot" running set of systems

3.2.2 Legacy Systems

DR for VA systems that are transitioning to virtualized or cloud environments is possible with a DRaaS solution. Typically, hardware and software will emanate from different suppliers and include different OSs, capacities, and services, thereby complicating a single solution for providing DRaaS.

For legacy or hybrid environments that include IT systems that have not migrated to a cloud environment, the following will be considered:

- How much of the infrastructure is comprised of operating systems that are capable of being part of an externally managed cloud-based DR solution?
- How many of the systems are capable of being virtualized?
- How many of the legacy systems will require co-located facilities to provide DR capability?
- Will the co-located facility be a VA facility or a commercially available facility?
- Are network requirements similar to those considered for a new system?

- Are technical limitations for DR identified in current DR Plan documentation (e.g., network connection difficulties and resultant testing requirements when new internet addresses are used by the legacy systems)?

A framework for the process that legacy systems should execute for a DRaaS solution will consist of the following:

- Identify the number of physical systems that can be virtualized and the required capacities that are capable of being supported by a cloud-based DR solution, including network and storage performance requirements
- Establish the RTO/RPO
- Establish the required data storage needed for backup, restoration and reconstitution of the systems data and applications. This includes Workload Transfer parameters which indicate how quickly static data and live workloads can be transferred; this has a direct impact upon how quickly VA can recover critical business processes
- Establish VA access and management needs for the systems, for both normal operations and in the event of a disaster
- Determine the FIPS 199 FISMA data classification (see 3.2.1)
- Determine the level of facilities required to support protection of the legacy system (see 3.2.1)

3.3 Challenges with DRaaS Solutions

An enterprise DRaaS solution would create uniformity for data recovery and mitigate risks (e.g., high data recovery costs), but not without potential challenges. As enterprise DRaaS solutions are assessed, VA will consider the following operational, performance, continuous service, and security challenges, as well as techniques to mitigate risks.

3.3.1 Operational

An operational risk with a DRaaS solution is the capacity strain of process-intensive systems, such as enterprise resource planning applications and VA relationship management systems on bandwidth. VA assets, such as backend reporting systems and databases, daily scheduled processes and systems, internal communication systems, and VA facing web applications can run on an Active-Active configuration with auto-failover. It is important to note that while DRaaS handles updating simple tasks well, process-intensive systems have an increased probability for network performance degradation. Constant updates to applications and VM images result in strained bandwidth for CSPs. CSPs often offer mock testing to illustrate a suitable bandwidth capacity; however, it is important to note that all clients are not included in the mock test. Therefore, results will not resemble an actual disruptive capacity. The most beneficial mitigation is to include a SLA clause to perform VA's own testing, rather than the conventional mock tests offered.

Vendor shortcuts also create DRaaS risks and downfalls. It is not cost effective for CSPs to build data centers that mimic the infrastructure of all of their customers. CSPs build their systems to handle a limited number of outages, making it clear that complete system redundancy does not exist. Lack of complete system redundancy can leave VA unaware of the CSPs true capabilities to provide quality and timely DR. A mitigation technique is to provide preference to DRaaS providers with geographically dispersed data centers and high levels of risk mitigation for failure events during the selection process.

3.3.2 Performance

A critical DRaaS solution attribute that can jeopardize recovery objectives is data movement performance. Data movement requires bandwidth and time, and both are dependent on the CSP's internet connection. A variety of reasons can stymie an internet connection and consequently delay daily backup and recovery strategies for VA. A mitigation strategy is to consider VA's network architecture, consider all data centers that will be impacted by data traffic, and prioritize VA failover systems in advance. These detailed planning and documentation measures will optimize productivity. VA's architectural assessment must consider identifying mission needs, VA policy, and security needs, which should be addressed in the SLA.

3.3.3 Continuous Service

SLAs should address the burden of proof when a vendor does not deliver services/capabilities continuously or at all, following an event. Although the fault of the outage is difficult to prove, due to the many network layers that may or may not be owned and or controlled by the CSP, the liability is with the CSP and not VA. A mitigation strategy is to use the SLA to explicitly identify roles and responsibilities during events that interrupt continuous service.

3.3.4 Security and Encryption

Specific security concerns on VA systems should be addressed appropriately in the SLA. VA systems contain PII for its employees and service members that are stored on Health Insurance Portability and Accountability Act (HIPAA) – compliant systems. As a result, it is imperative that the CSP's site meets all FIPS, FISMA and VA security requirements, as well as the CSP's supply chain. Note that a CSP's supply chain may have its own required security standards, which may or may not be aligned to VA standards. A mitigation strategy that ensures that all VA required security measures are appropriately implemented, VA must do its due diligence in vetting the CSP supply chain culture for security.

3.4 Alignment to the One-VA Technical Reference Model (TRM)

All projects will leverage the approved technologies and standards included in the One-VA Technical Reference Model (TRM)[6] in order to comply with the architectural guidance provided by this authoritative source from the VA production computing environment. Table 3 lists the approved tools for this EDP.

Table 3: List of Approved Tools and Standards for Enterprise Authorization

Tool Category	Example Approved Technologies
Disaster Recovery	CA Copycat, EMC Data Domain Operating System (DD OS), EMC Data Domain Replicator (DD Replicator), Enterprise Library Software (ELS), InMage Scout, Red Hat Enterprise Virtualization (Servers), Sustainable Planner, Veeam Backup & Replication, Veritas Cluster Server (VCS), VMware Site Recovery Manager (SRM), VMware vCenter Server Heartbeat, VMware vSphere
Cloud Technologies	CloudForms, EMC Atmos GeoDrive, iCloud, Heroku, OpenShift Enterprise, OpenStack, Cloud Foundry, and Azure

3.5 Alignment to Veteran-Focused Integration Process (VIP)

All projects subject to the Veteran-Centric Integration Process (VIP) will leverage enterprise services to support DR instead of implementing a custom DR solution. VIP is a Lean-Agile framework that serves the interest of Veterans through efficiently streamlining activities that occur within the enterprise. The VIP framework unifies IT delivery oversight and will deliver IT products more securely and predictably. VIP is the follow-on framework from the Project Management Accountability System (PMAS) for the development and management of IT projects; it will propel VA with even more rigor toward the Veteran-focused delivery of IT capabilities.

[6] http://trm.oit.va.gov/

More information can be found here (https://vaww.oit.va.gov/veteran-focused-integration-process-vip-guide/).

4 USE CASES

4.1 Utilizing a DRaaS Solution for a Virtual Environment

4.1.1 Purpose

The purpose of this use case is to illustrate how VA can leverage several built-in features of a DRaaS solution to meet data protection and recovery needs in a VA virtual environment. It is important to recognize that while the scenario for this Use Case is a FISMA moderate three-tier DRaaS solution. DRaaS solutions also have the capability to effectively address FISMA High critical system RTO requirements of zero downtime, with its fully automatic redundant support, using an Active-Active configuration.

4.1.2 Assumptions

- VA environment is virtual and provides rapid scaling and failover
- VA has identified virtual critical resources and systems through BIA and DR planning
- VA RTO and RPO for critical virtual systems were identified
- Replication policies are in place for VA infrastructure
- The VA virtualized infrastructure can handle the high level of internal demand that is necessary for operations
- Static web content, logs, and snapshots are included in the virtual infrastructure

4.1.3 Use Case Description

A VA public-facing web application encountered an interruption. The application is a FISMA moderate three-tier with a RTO for greater than one day. The VA backup and restore is a multi-site cloud and on premise architecture. The system must become operational within the required amount of time. The configuration shown in Figure 2 is based on a representative industry best practice use case from a VA partner such as Amazon.

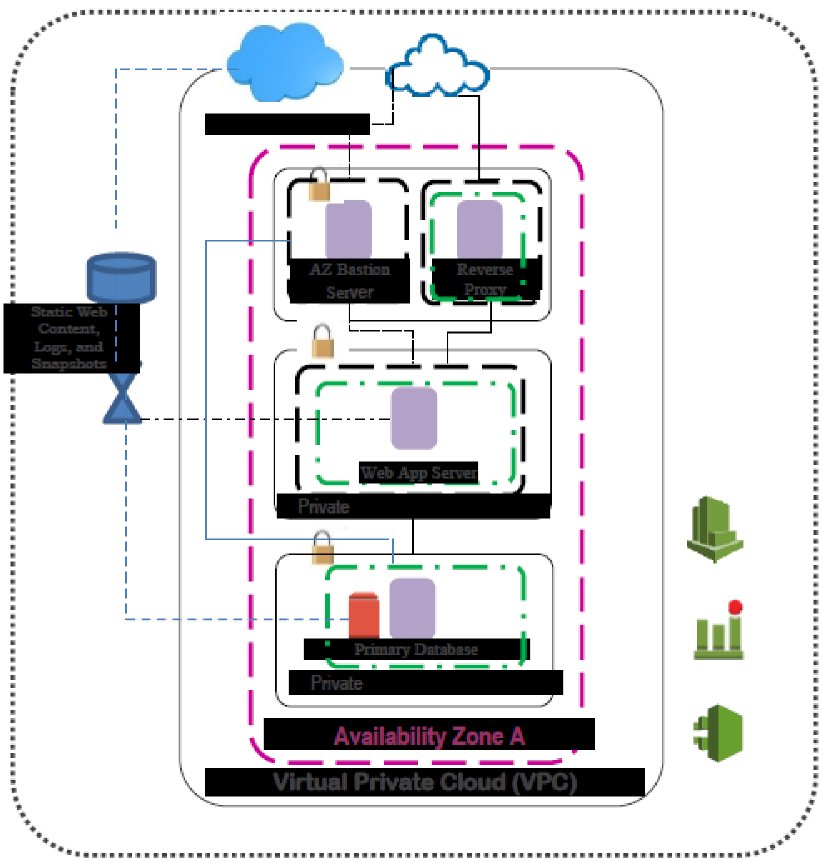


FIGURE 2: EXAMPLE OF DRAAS CONFIGURATION FOR A VIRTUAL ENVIRONMENT

Step 1

Prior to any interruption, backups take place. VA's web application server deduplicates, compresses, and encrypts the changed blocks of VMs. It then transmits this data to the DRaaS provider's data center.

Step 2

From the DRaaS provider's data center, VA data is placed in the cloud. The data is built from the foundation of primary data built out for DR.

Step 3

A replication of what is on premise would be built with the database server, web and application tier, reverse proxy, and web server. This can be constructed entirely in a cloud environment using restored data.

Step 4

When an interruption occurs, the VMs can be powered up and accessed by external Internet Protocol (IP) access. This is possible because data already exists on "standby." With the restored data resting in the cloud, the system could be operational in a day and meet the greater-than-one-day RTO.

Step 5

When the disaster causes interruption, the remote VA backups increase the changed blocks of VMs at the data center. The changed VMs are then restored to the original infrastructure when all systems are back online.

4.2 Utilizing a DRaaS Solution for a Legacy Environment

4.2.1 Purpose

The purpose of this use case is to outline a scenario that a VA project team might consider when it has been determined that a hybrid cloud-based DRaaS capability is appropriate for the backup, protection, and retention of critical data and applications for a legacy environment.

4.2.2 Assumptions

- All required federal and VA regulations required have been identified
- RPO and RTO for data and application recovery have been established
- The BIA for DR planning has been referenced
    - Detailed technical requirements for data and applications recovery have been identified in the event of a disaster
    - The necessary data security accessibility and integrity requirements have been identified and established and conveyed
- On-premise virtualization of servers is part of the hybrid data backup and recovery scenarios to be considered
- Sufficient data recovery capacity required of a CSP and on premise storage has been identified

Technical Considerations

For a hybrid cloud-based scenario, VA would need to determine the necessary data protection requirements for systems and applications residing in a commercial cloud environment. Other technical requirements to consider include:

- The internet bandwidth required at Information Technology Center (ITC) for the commercial cloud provider to allow data to be backed up or replicated
- The storage space that is required at the commercial cloud data center, including the number of virtual servers and VMs needed for virtualization
- How to integrate with existing enterprise systems
- Determining How existing business applications, management, and monitoring systems can be leveraged
- The level of control over the solution VA requires and negotiate those requirements with the commercial cloud and colocation providers
- The requirements for frequency of testing within the hybrid cloud-based or collocated solution

It is vitally important to verify that the commercial cloud provider adheres to VA and federal regulatory and compliance requirements to include data placement, data encryption, personal information protection, and contractual management (e.g., software licensing).

4.2.3 Use Case Description

This use case describes a hybrid on premise to CSP backup and data recovery configuration. It outlines an example of a FISMA moderate configuration, with a RTO that is less than or equal to one hour. The configuration shown in Figure 3 is based on a representative industry best practice use case from a VA partner, such as Amazon.

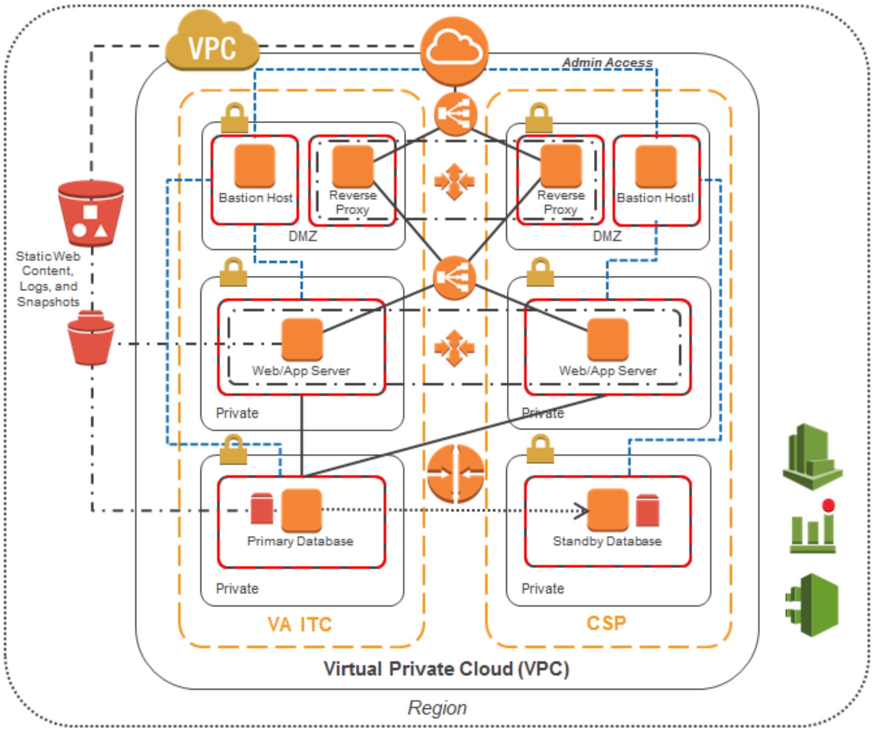


FIGURE 3: EXAMPLE OF A HYBRID CLOUD-BASED DRAAS CONFIGURATION

Step 1

Verify that all the infrastructure components (web servers, application servers, storage devices, communications devices and Active Directory) are housed in the VA ITC data center and configured in the CSP infrastructure components.

Step 2

Utilize an API in a VA backup and archiving software application or a CSP-provided gateway for VA connectivity to securely store data in the cloud. This provides data encryption, as well as scalable and cost-effective storage for recovery.

Step 3

Verify that the requirement for a secure network connection exists between the VA ITC and CSP has been established. This is accomplished with a direct connection or through a secure virtual private network (VPN) connection. Using this method, VA backups and archives are automatically offsite (for compliance purposes) and stored on durable media, eliminating the complexity and security risks of off-site tape management. Well-designed and secure data protection solutions typically use a combination of cloud-native and on-premises solutions.

APPENDIX A. SCOPE

This EDP is a supporting guidance document for VA for the use of DRaaS. This EDP provides guidance on identifying DRaaS capabilities within the VA enterprise and integrating DRaaS with existing VA services. This document will also refer to other cloud computing and IT Service Management (ITSM) EDPs, in order to highlight required supplemental activities when using DRaaS.

Topics that are out of scope for this EDP, but may be referenced, are:

- Business Continuity
- Cloud Security
- Contingency Planning
- DR Planning
- DRP development

Document Development and Maintenance

This EDP was developed collaboratively with internal stakeholders from across VA, including participation from subject matter experts (SMEs) from OI&T pillars, including the Enterprise Program Management Office (EPMO), the Office of Information Security (OIS), Architecture, Strategy and Design (ASD), and Service Delivery and Engineering (SDE). Extensive input and participation was also received from Veterans Health Administration (VHA), Veterans Benefits Administration (VBA), and National Cemetery Administration (NCA). In addition, the development effort included engagements with industry experts to review, provide input, and comment on the proposed pattern. This document contains a revision history and revision approval logs to track all changes. Updates will be coordinated with the Government lead for this document, which will also facilitate stakeholder coordination and subsequent re-approval, depending on the significance of the change.

APPENDIX B. DEFINITIONS

This appendix provides definitions for terms used in this document, particularly those related to databases, database management, and data integration.

Key Term	Definition
Business Continuity Planning (BCP)	The documentation of a predetermined set of instructions or procedures that describe how an organization's mission/business processes are sustained during and after a significant disruption.
Business Impact Analysis (BIA)	An analysis of an information system's requirements, functions, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption.
Contingency Planning	Management policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disasters. Information system contingency planning refers to the dynamic development of a coordinated recovery strategy for information systems, operations, and data after a disruption.
Disruption	An unplanned event that causes an information system to be inoperable for an unacceptable length of time (e.g., minor or extended power outage, extended unavailable network, or equipment or facility damage or destruction).
Disaster Recovery Plan (DRP)	A written plan for recovering one or more information systems at an alternate facility in response to a major hardware or software failure or destruction of facilities. The DRP is supported by the information system contingency plans (ISCPs) for each critical IS Service at the affected facility.
Information System (IS)	An assembly of computer hardware, software, or firmware configured to collect, create, communicate, compute, disseminate, process, store, and control data or information. An information system will consist of automated data processing system hardware, operating system and application software, peripheral devices, and associated data communications equipment.

Key Term	Definition
Recovery Site	A location, other than the systems primary location, used to continue operational capabilities during a significant system disruption.
System	A generic term used for briefness to mean either a major application or a general support system.
User	A person who accesses information systems to use programs or applications in order to perform an organizational task.

APPENDIX C. ACRONYMS

The following table provides a list of acronyms that are applicable to and used within this document.

Acronym	Description
API	Application Programming Interface
ASD	Architecture Strategy and Design
BCP	Business Continuity Plan
BIA	Business Impact Analysis
CapEx	Capital Expenditure
CIA	Confidentiality, Integrity, and Availability
CIO	Chief Information Officer
CSP	Cloud Service Provider
DR	Disaster Recovery
DRaaS	Disaster Recovery as a Service
DRP	Disaster Recovery Plan
EDP	Enterprise Design Pattern
EPMO	Enterprise Program Management Office
ETA	Enterprise Technical Architecture
FedRamp	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
HIPAA	Health Insurance Portability and Accountability Act
IP	Internet Protocol
IT	Information and Technology
ITC	Information Technology Center
ITSM	Information Technology Service Management
KPI	Key Performance Indicator
NCA	National Cemetery Administration
NIST	National Institute of Standards and Technology
OIS	Office of Information Security
OI&T	Office of Information and Technology
OpEx	Operational Expenditure
OS	Operating System
P-ATO	Provisional Authority to Operate
PII	Privacy and Personally Identifiable Information
PMAS	Project Management Accountability System
PMEF	Primary Mission Essential Function
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SDE	Service Delivery and Engineering

Acronym	Description
SLA	Service Level Agreement
SME	Subject Matter Expert
TRM	One-VA Technical Reference Model
VA	Veterans Affairs
VBA	Veterans Benefits Administration
VHA	Veterans Health Administration
VIP	Veteran-Centric Integration Process
VistA	Veterans Health Information Systems and Technology Architecture
VM	Virtual Machine

APPENDIX D. REFERENCES, STANDARDS, AND POLICIES

This EDP is aligned to the following VA OI&T references and standards applicable to all new applications being developed in the VA, and are aligned to the VA Enterprise Technical Architecture (ETA):

#	Issuing Agency	Policy, Directive, or Procedure	Purpose
1	VA	VA Directive 6551	Establishes a mandatory policy for establishing and utilizing Enterprise Design Patterns by all Department of Veterans Affairs (VA) projects developing information technology (IT) systems in accordance with VA's Office of Information and Technology (OI&T) integrated development and release management process, the Veteran-focused Integration Process (VIP).
2	VA OIS	VA 6500 Handbook	Directive from the OI&T OIS for establishment of an information security program in VA, which applies to all applications that leverage ESS
3	VA OIS	VA Directive 6517	Establishes policy, roles and responsibilities regarding evaluation for selection of secure cloud computing services for VA; also establishes VA policy for compliance with the Federal Chief Information Officer's (CIO) mandate for a 'Cloud First' policy; the CIO's policy is intended to accelerate the pace at which the government will realize the value of cloud computing by requiring agencies to evaluate safe, secure cloud computing options before making new technology investments

Disclaimer: This document serves both internal and external customers. Links displayed throughout this document may not be viewable to all users outside the VA domain. This document may also include links to websites outside VA control and jurisdiction. VA is not responsible for the privacy practices or the content of non-VA websites. We encourage you to review the privacy policy or terms and conditions of those sites to fully understand what information is collected and how it is used.