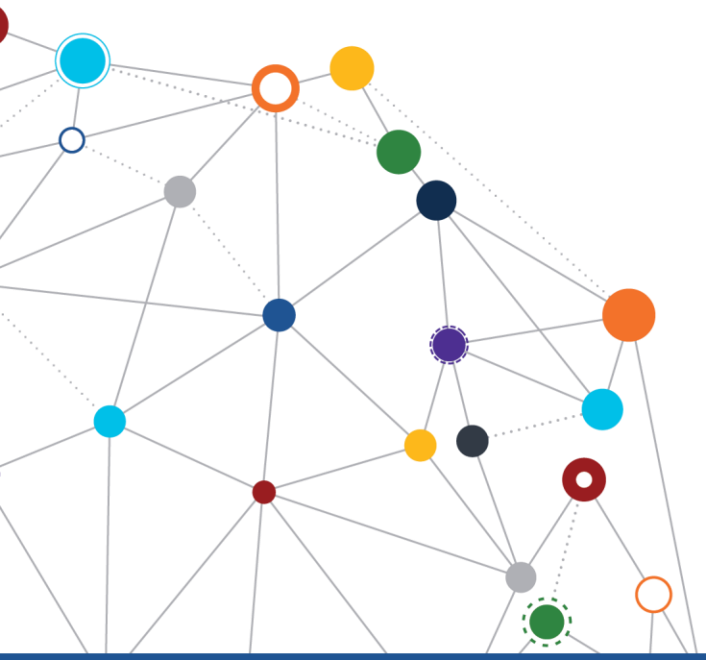
OFFICE OF
INFORMATION
AND TECHNOLOGY

Infrastructure-as-a-Service (IaaS) Enterprise Design Pattern

IaaS Use Case - Data Center Virtualization

August 2018 | Demand Management Division



VA

U.S. Department of Veterans Affairs
Office of Information and Technology

Table of Contents

1 Context 3
2 Problem 3
3 Approach 3
3.1 IaaS Considerations 3
4 Application 4
4.1 Data Center Virtualization 4
4.1.1 Purpose 4
4.1.2 Assumptions 5
4.1.3 Use Case Description 5
4.2 DEA User Stories 9
5 Impacts 11
Appendix: References 12

Figure 1: Data Center Virtualization 8

Table 1: Change Matrix 2
Table 2 : Guiding Principles IaaS EDP 9

Table 1: Change Matrix

Version	Date	Description of Updates
1.0	08/03/2018	IaaS EDP Segment 3 document approved

1 Context

The move to an Infrastructure-as-a-Service (IaaS) model enables the Department of Veterans Affairs (VA) to achieve economies of scale, greater elasticity, greater resource efficiency, and better ability to maintain systems. IaaS breaks down data center silos, for example, by moving systems to the cloud. When management groups do not share information, goals, tools, priorities, and processes with each other, duplication and redundancy are at risk.

2 Problem

Project teams at VA would benefit from example scenarios with goals, decisions points, and an end state that mirrors the situations that they could encounter with IaaS based projects. The IaaS EDP Use Case provides project teams at VA with events that will further inform and prepare them, such as industry best practices, corresponding internal VA resources and references, and applicable guidance from previous EDPs. The Enterprise Cloud Solution Office (ECSO) Team works with project managers and business owners to determine an application's suitability for the VA Enterprise Cloud (VAEC). The IaaS EDP Use Case includes the resources and guidance of the VAEC.[1]

3 Approach

The VAEC offers on-demand self-service, broad network access, resource pooling, elasticity, and a measured service. Currently, the VAEC provides private VA cloud environments in the Amazon Web Services (AWS) Government Cloud and the Microsoft Azure Government Cloud (MAG). VA is also planning an on-premise VA Private Cloud.[2]

3.1 IaaS Considerations

The VA mission and vision should be driving the selection of the cloud service provider (CSP), rather than a technology or platform acting as the basis for the choice of CSP. The following guidance can assist in determining the CSP and preparing for IaaS migration.

- The CSP selection decision should be informed by the VA Enterprise Architecture (EA), which guides and constrains the technical implementation of VA's mission and vision. The VA EA Team is collaborating with Enterprise Cloud Solutions Office (ECSO)[3] to converge on guidance for the CSP selection process for a given application platform migration.

[1] Reference the Cloud First Policy, articulated within VA Directive 6517, *Cloud Computing Services*, at http://www.va.gov/vapubs/viewPublication.asp?Pub_ID=852&FType=2.
[2] Reference additional information on the VAEC at https://vaww.portal.va.gov/sites/ECS/SitePages/VA-Enterprise-Cloud-VAEC.aspx.
[3] The VAEC is supported by the Enterprise Cloud Solutions Office (ECSO) and implements the VA Cloud-First Policy that is articulated in VA Directive 6517, *Cloud Computing Services*.

Project teams should consult the VA EA Website for the most current information, when it has been made available.[4]

- Some systems may not be appropriate for migration; these systems may need to be divested because they are duplicative or no longer support the mission, or are obsolete and not aligned with VA's vision.[5] An example of these is found in legacy systems that run on a mainframe or unsupported platform, such as the Business Delivery Network (BDN) suite of systems.
- Project managers must consider the interdependencies among systems when moving to the IaaS Cloud. The following represent requirements for a successful IaaS transition:
  - The system must have a similar architecture to the destination cloud.
    - The Cloud Operating System (OS) must be determined. The accurate OS for the environment will be transitioned and can be confirmed with the Data Center Lead or Technical SME for the site.
  - Networks, storage, virtualization, and servers are managed by the vendor; however, software and related tasks (e.g., OS, middleware, runtime, data, and applications) are managed by the VA customer. For project teams, this means having staff with the skills needed to perform the tasks, and the experience needed for managing the resources that are not covered by the IaaS CSP.
  - It is necessary to include a team of Government SMEs on staff during the IaaS transition to maintain experienced personnel, with familiarity of the OS and applications that will be transitioned.

4 Application

The following use case represents IaaS data center utilization.

4.1 Data Center Virtualization

4.1.1 Purpose

The use case provides an example of how VA can move from dedicated data centers to virtualized data centers in the cloud.

[4] Reference the VA Enterprise Architecture at https://www.ea.oit.va.gov/.
[5] Reference additional information on sunsetting legacy applications at the *Transition to Cloud* EDP at https://www.oit.va.gov/library/programs/ts/edp/cloud/TransitiontoCloud_V1.pdf.

4.1.2 Assumptions

- Security requirements for integrating with Cloud Services are met by means of the Federal Risk and Authorization Management Program (FedRAMP)[6] and the VA Cloud Security Handbook.[7]
- The VAEC has been deployed and is in use to manage the Cloud Services that are consumed by VA.
- The application starts in a non-cloud environment and moves to the VAEC.
- The application cannot be taken down for maintenance.

4.1.3 Use Case Description

1. Perform an analysis of current design. In IaaS, project teams will be responsible for applications, data, runtime, middleware, and O/S, utilizing a Business Impact Analysis (BIA).[8]
    - Conduct a BIA to correlate information systems with critical mission/business processes:
        - Utilize the VA System Inventory (VASI).[9] The VASI is the authoritative data source for VA IT systems and is a vital component of the Department's Enterprise Architecture. This System or Record (SOR) is a department-wide inventory of systems and systems-related information, and provides the current state of VA's IT environment. Risk management analysis validates these systems before inclusion in the VASI SOR. The systems then receive an Authority to Operate (ATO). This validation process provides a departmental process for conducting both risk management and BIA.
        - Determine which systems are vital. All mission-critical systems directly support one of VA's mission essential functions (MEFs).[10] Therefore, all resources deemed "vital" require a BIA. This includes IT systems that support Veterans and clinicians; and systems, devices, and processes which aid communication in the event of a disaster. Systems that aid in identifying and treating patients under Veterans Health Administration's (VHA) direct care are also required to complete a BIA.

---

[6] Reference FedRAMP at https://www.fedramp.gov/.
[7] Reference the VA *Cloud Security Handbook*, VA Directive 6517, at https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=853&FType=2.
[8] Reference the *Business Impact Analysis* EDP at https://www.oit.va.gov/library/programs/ts/edp/itsm/BusinessImpactAnalysis_V1.pdf.
[9] Reference the VASI Dashboard at http://vaausappdar401.aac.dva.va.gov/views/VAEATargetPortfolios/VATargetPortfolioDashboard?:iid=1&:isGuestRedirectFromVizportal=y&:embed=y.
[10] VA's Mission Essential Functions (MEFs) are described in Appendix A, page 18, VA Handbook 0322 at https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=582&FType=2.

        - Assess the likelihood of failure, recovery options, and/or replacement options.
2. Establish the feasibility of cloud solutions; determine if virtualization, servers, storage, and networking can be abstracted away by the CSP. DECISION: if no, then return to step 1, otherwise continue utilizing Cloud Architecture[11]
    - For cloud architecture, it is important to note how users will develop and leverage cloud-based resources to meet the VA user needs:
        - Access the applications through web, mobile, desktop, or hybrid environments.
        - Account for the number of users and their locations.
        - Ensure applications and that services will scale with users or workload.
        - Enable notifications, such as e-mail, SMS, or mobile.
3. Determine which VAEC cloud to use.
4. Conduct capacity planning, utilizing Application Performance Management (APM).[12]
    - Apply APM capabilities to evaluate applications and proactively identify risks.
        - Trend and analyze: Establish comprehensive capacity management planning practices.
        - Resolve application incidents and outages; allow more effective use of the monitoring tool infrastructure through active capacity reporting and planning.
5. Develop requirements for main and redundant systems, utilizing Disaster Recovery-as-a-Service (DRaaS).[13]
    - Select enterprise DRaaS to support Disaster Recovery (DR).
        - Determine DR configuration by assessing key attributes for recovery capabilities:
            - The period of acceptable downtime and level of data loss: Key performance indicators (KPIs) include specific Recovery Point Objective (RPO)/Recovery Time Objective (RTO).
            - Prioritization of environments and systems are based on mission criticality.
            - Recovery Capabilities: The following features should be available in the DRaaS solution and are determined by the RTO and RPO:
                - DR Standby Operational Scenarios (cold sites, warm sites, hot sites, mirrored sites)

[11] Reference the *Cloud Computing Architecture* EDP at https://www.oit.va.gov/library/programs/ts/edp/cloud/CloudComputingArchitecture_V1.pdf.
[12] Reference the *Application Performance Management* EDP at https://www.oit.va.gov/library/programs/ts/edp/ea/ApplicationPerformanceManagement_v3.pdf.
[13] Reference the *Disaster Recovery as a Service* EDP at https://www.oit.va.gov/library/programs/ts/edp/itsm/DisasterRecoveryAsAService_V1.pdf.

- DR types (simple backup solution with integrated offsite/cloud capabilities, hybrid, integrated/orchestrated, mission critical)

6. Assess existing maintenance agreements for data center. Does the CSP lay out the clear responsibilities for virtualization, servers, storage, and networking? DECISION: if no, return to step 1.
7. Establish Service Level Agreements (SLAs), utilizing Cloud Security.[14]
    - For cloud security (additional details can be found in Handbook 6500)[15]:
        - Trusted Internet Connection (TIC) compliance: Ensure cloud projects are TIC compliant, decreasing network security risks.
            - Internal applications do not need to comply with TIC.
            - External applications must comply with TIC.
        - Strong cloud controls: Provide guidance for minimizing risk while VA controls are in development.
        - Protect sensitive data: Identify when and how encryption can mitigate cloud risks.
            - Data in transit – encryption available
            - Data at rest – encryption available
            - Data in use – encryption unavailable
        - Cloud visibility: Set expectations for audit logging goals to create cloud visibility:
            - Create an Authorized User List.
            - Set up a Network Access Control Table.
            - Log monitors in the Network Access Control Table.
        - Cloud availability: Identify major challenges for consideration to reduce risk that is related to cloud service availability.
8. Utilize VAEC monitoring.
9. Produce alerts for VAEC.
10. Generate test plan.
11. Establish the virtualization infrastructure within the VAEC.
12. Design, validate, and plan the virtualization; DECISION: if no, return to step 7.
13. Backup systems, including redundant systems to redundant cloud, prior to virtualization.
14. Conduct virtualization for main and redundant system.
15. Ensure monitoring and alert systems are actively functioning.
16. Close out previous data center.

[14] Reference the *Cloud Security* EDP at https://www.oit.va.gov/library/programs/ts/edp/privacy/CloudSecurity_V1.pdf.
[15] Reference Handbook 6500, *Risk Management Framework for VA Information Systems*, at https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=793&FType=2.

This high-level process flow is depicted in the flowchart that follows. These steps represent IaaS tasks that are the responsibility of the project teams and may not be covered by the CSP.

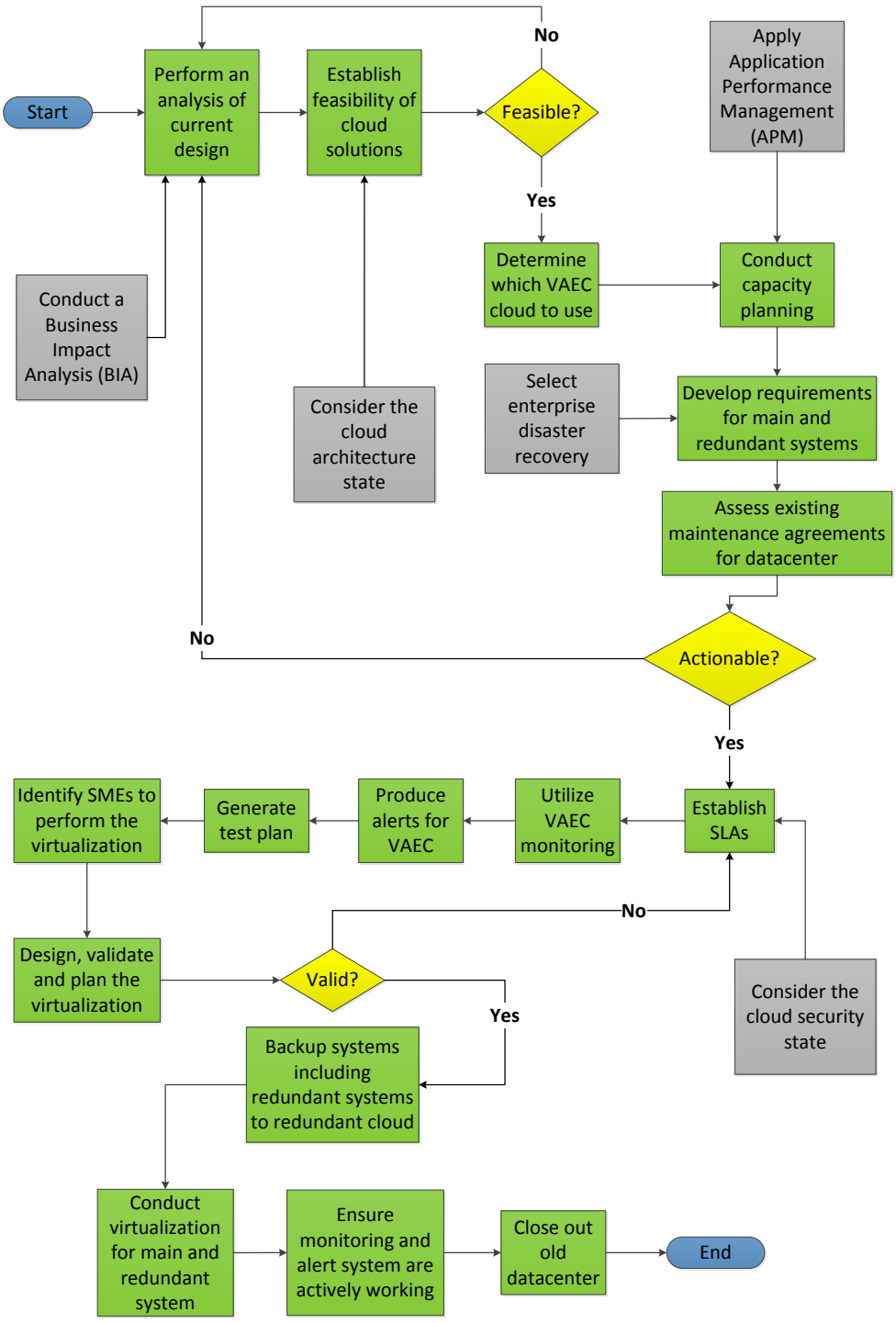


Figure 1: Data Center Virtualization

4.2 DEA User Stories

Project teams using the Veteran-focused Integration Process (VIP) must comply with the approved standards in the One-VA TRM;[16] and map to the Design, Engineering, and Architecture (DEA) user stories below. The DEA user stories have a standard for IaaS utilization.

Table 2 : Guiding Principles IaaS EDP

DEA User Story	Title	User Story Text	Relevant User Story Acceptance Criterion
DEA 04.21.02	Infrastructure Capacity	As an enterprise architect, I need a scalable infrastructure to ensure that capacity meets the needs for VA IT systems.	(1)-Workload/performance testing is conducted and results are documented. The resulting data are compared to previous performance baselines and provided to organizations supporting enterprise operations and/or field operations for review and action, as needed. (2)-Completed infrastructure capacity assessment, which includes assessment of capacity requirements and impact analysis, based on the SLA where one exists. (3)-Where applicable, Wide Area Network (WAN) monitoring and analysis are completed for any project iteration that introduces changes, with the potential to impact network resources or end-user response time. Potential impact is determined by measured changes in transaction size and volume, resulting from the iteration feature improvements. (4)-Performance testing and monitoring documentation is provided, if available in the SLA,

[16]Reference the One-VA TRM from the internal VA network at http://trm.oit.va.gov/.

DEA User Story	Title	User Story Text	Relevant User Story Acceptance Criterion
			between the project team and hosting provider, or other design documentation.
DEA 04.21.03	Scalability	As an enterprise architect, I need scalability so that VA systems and services resource pools can expand and contract to meet demand, optimizing cost and access.	(1)-The solution components are designed to scale out and to operate on a series of loosely coupled commodity platforms; the solution is verified to scale-out without requiring code changes.
DEA 04.23.02	Virtualization	As an enterprise architect, I need virtualization, so that VA systems are independent of physical infrastructure, ensuring flexible environments that are scalable and quickly deployed.	(1)-The solution design, platform requirements (i.e. operating system), and software components have been shown to be compatible with current enterprise virtualization technologies by setting a precedent for direct testing, or other reasonable methods.
DEA 04.21.02	Storage	As an enterprise architect, I need storage, so that infrastructure can support VA applications.	(1)-Storage capacity requirements are established and documented, based on capacity analysis and/or models.
DEA 04.21.01	Compute Capacity	As an enterprise architect, I need Compute Capacity Testing, so that capacity changes can be detected and resolved.	(1)-A documented test solution exists for any project iteration that introduces changes with the potential to impact end-user performance, or computer and storage resources.

5 Impacts

If a move to the IaaS Cloud is not implemented, the following are potential pitfalls:

- Higher capital expenditure costs (CapEx)
- Lower computing power because servers in the VAEC are tuned for high performance, availability
- Less scalability

Appendix: References

References:

- Application Performance Management EDP: https://www.oit.va.gov/library/programs/ts/edp/ea/ApplicationPerformanceManagement_v3.pdf
- Business Impact Analysis EDP: https://www.oit.va.gov/library/programs/ts/edp/itsm/BusinessImpactAnalysis_V1.pdf
- Cloud Computing Architecture EDP: https://www.oit.va.gov/library/programs/ts/edp/cloud/CloudComputingArchitecture_V1.pdf
- Cloud First Policy: http://www.va.gov/vapubs/viewPublication.asp?Pub_ID=852&FType=2
- Cloud Security EDP: https://www.oit.va.gov/library/programs/ts/edp/privacy/CloudSecurity_V1.pdf
- DEA User Stories: https://vaww.portal2.va.gov/sites/asd/TechStrat/IPTS/SitePages/Home.aspx
- Disaster Recovery as a Service EDP: https://www.oit.va.gov/library/programs/ts/edp/itsm/DisasterRecoveryAsAService_V1.pdf
- ECSM EDP: https://www.oit.va.gov/library/programs/ts/edp/cloud/EnterpriseCloudServiceManagement_v2.pdf
- ECSO Service Request: https://vaww.portal.va.gov/sites/ECS/SitePages/ECS-Request-Form.aspx
- FedRAMP: https://www.fedramp.gov/
- Handbook 6500: https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=793&FType=2
- Transition to Cloud EDP: https://www.oit.va.gov/library/programs/ts/edp/cloud/TransitiontoCloud_V1.pdf
- TRM: http://trm.oit.va.gov/
- VA Available Cloud Training: https://vaww.portal.va.gov/sites/ECS/SitePages/Cloud-Training.aspx
- VA Cloud Security Handbook, VA Directive 6517: https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=853&FType=2
- VA Cost Benefit Analysis Template: https://www.va.gov/PROCESS/artifacts/cost_benefit_analysis_template.docx

- VA Digital Modernization Strategy, April 11, 2018 VA Directive 6551: https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=829&FType=2
- VA Enterprise Architecture: https://www.ea.oit.va.gov/
- VA MEFs: https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=582&FType=2
- VAEC: https://vaww.portal.va.gov/sites/ECS/SitePages/VA-Enterprise-Cloud-VAEC.aspx
- VASI Dashboard: http://vaausappdar401.aac.dva.va.gov/views/VAEATargetPortfolios/VATargetPortfolioDashboard?:iid=1&:isGuestRedirectFromVizportal=y&:embed=y
- VEAR: https://vaausdarapp82.aac.dva.va.gov/ee/request/home

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.

Statement of Endorsement: Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, and shall not be used for advertising or product endorsement purposes.