National Institute of
Standards and Technology
U.S. Department of Commerce

USAID VDI in the Cloud

A Cloud Computing Use Case

Version 1.2 - DRAFT

Document Revision History

Revision	Date	Change	Author	Company
V1.0	2/23/2011	Initial Creation	Viktor Kaufmann	Knowcean Consulting
			Jin Tong	Knowcean Consulting
			Jian Mao	Knowcean Consulting
V1.1	3/22/2011	General edits, new diagram, inserted security discussion of deployment models.	Viktor Kaufmann	Knowcean Consulting
			Jin Tong	Knowcean Consulting
V1.2	3/29/2011	Added disclaimer.	Viktor Kaufmann	Knowcean Consulting

Disclaimer

This document has been prepared by the National Institute of Standards and Technology (NIST) and describes standards research in support of the NIST Cloud Computing Program. Certain commercial entities, equipment, or material may be identified in this document in order to describe a concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that these entities, materials, or equipment are necessarily the best available for the purpose.

DRAFT

Table of Contents

Disclaimer 2
Description 4
Background 5
Cloud Computing Concept of Operations 5
Analysis 7
Service Model 7
Deployment Model 8
Cloud Computing Essential Characteristics 8
On-demand self-service 8
Broad network access 8
Resource pooling 8
Rapid elasticity 8
Measured service 8
Security 9
Interoperability 9
Portability 9
Maintainability 10
Usability 10
Performance 11
Resilience 11
Concerns and Challenges 11

DRAFT

Description

The U.S. Agency for International Development (USAID) is interested in going to cloud to provide IT services for its users distributed across the globe. The initiative is to move applications such as email, office productivity and some business applications into clouds and implement a cloud-based VDI to enable secure access to the cloud-based services.

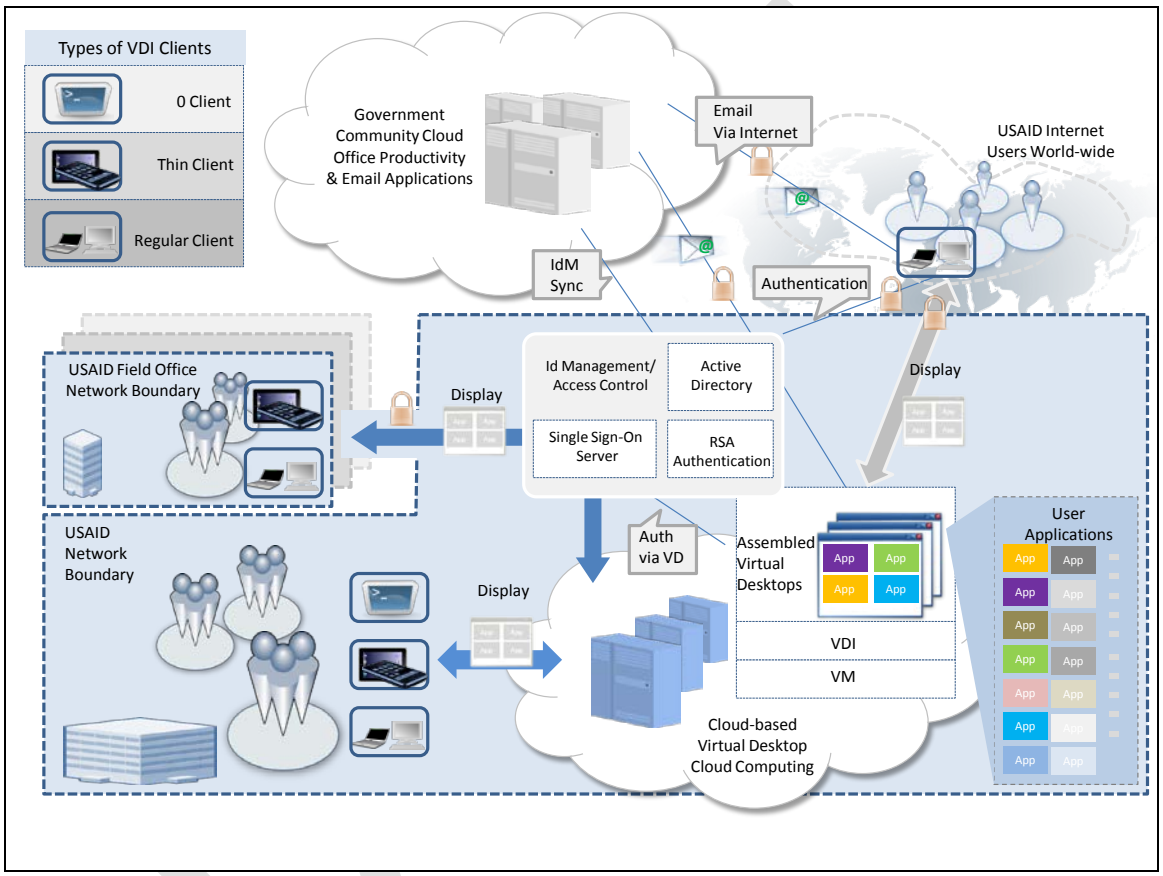

Figure 1: USAID Cloud Implementation Overview

Background

USAID has approximately 8,000 users worldwide using 3,739 identified applications. Users generally use desktops with standard images without administrative rights, preventing installation of applications that have not been approved by the IT department. Few laptops have been deployed due to security requirements to prevent data loss. When users travel, they normally carry hardcopy documents rather than using laptops (recently iPads were introduced to mitigate this, encrypting data rather than devices). Remote access to computer resources for purposes such as telecommuting is enabled using a Citrix solution.

Within USAID there is dissatisfaction with the lack of flexibility within the IT services offered, an inability to access some IT resources while fulfilling day-to-day mission tasks, and a general desire to see technologies made available across the organization. In addition to complaints about mailbox quotas negatively impacting productivity, there is a great deal of dissatisfaction among users about the lack of accessibility outside of mission offices, leading some users to utilize external workarounds such as web-based mail. Limited and unreliable access at remote sites is a significant concern for users in the field, and IT policies affecting available services contribute to that.

The USAID Office of Chief Information Officer (OCIO) has limited visibility into IT resources and applications used outside of the main offices, especially at the field missions. By implementing VDI and gradually moving applications into the cloud and enabling the deployment of new applications in the cloud, USAID OCIO anticipates gaining visibility into how their users actually use these applications.

Cloud Computing Concept of Operations

USAID is interested in going to cloud to provide IT services for its users distributed across the global. The planning is to move applications such as email, office productivity and some business applications into clouds and implement a cloud-based VDI to enable secure access to the cloud-based services. The main reasons to pursue this are to decrease the cost of delivering computing and support services, creating a mobile workforce able to use a variety of devices, and improving security by limiting the loss of sensitive data through the loss or theft of a mobile device or by malicious software. Specifically, the VDI will reduce the high cost associated with providing and maintaining desktop service, and by moving IT services into the cloud help to reduce the need and the cost associated with developing and maintaining data centers. USAID expects a hybrid cloud environment that uses both private cloud and community cloud for its cloud effort.

As seen in Figure 1, USAID's cloud-based VDI will be deployed in a private cloud with clients being able to access the VDI and the cloud-based applications. The security infrastructure that

enables single-sign-on and two factor authentication is also an essential part of the solution and will be deployed in the same private cloud.

The VDI consists of desktop virtualization solutions and Citrix servers deployed on virtual machines. The desktop virtualization solution (e.g., AppSense solutions at USAID) enables personalized standard virtual desktops by automatically applying policy and personalization data to the desktop on demand. Desktop virtualization enables hosting of individual desktops inside virtual machines. When a user logs in through the single sign-on infrastructure with two factor authentication (e.g., Ping identity management product/RSA SeCurID and Active Directory), a secure virtual user desktop with an application work group is presented to the user on whatever device the user connected through. Applications and privileges made available in the workgroup are determined by the group profile assigned

Three types of client devices are expected to be issued to users in the USAID offices: zero clients, thin clients, and regular workstations, with the goal being to migrate toward zero clients and no data stored locally.

a) zero client - Wyse device;
b) thin client - devices such as IPAD with memory to support applications that may require video processing.
c) regular workstations.

In most cases, all computation is handled on the server side. Thin clients with local memory help to reduce the number of Citrix servers required to host desktops where that requires significant computing power (for example, video processing). Unlike traditional desktops and laptops, all storage would be network-based, eliminating the need for data encryption on the device. As data are no longer stored on the device at all, data would no longer be compromised in the event of a theft or loss of a device. The same secure virtual desktop will be presented whenever/wherever the user is logged into the VDI.

USAID has identified fifty applications that would be virtualized and streamed in the initial phase of implementing VDI out of its portfolio of 3,739. Other applications would be reviewed and gradually migrated to the cloud if the same functions could not be provided by existing approved applications.

User virtualization would be used to allow personalization of virtual desktops by the end user regardless of the desktop and application delivery technologies and platforms. The increased visibility into the USAID application portfolio would allow greater standardization on applications. Delinking the desktop from the device increases flexibility by allowing users to select among a variety of computing devices and enabling the use of these devices anywhere.

The use of virtual machines simplifies and speeds up user provisioning and de-provisioning. While many of the same steps need to be followed in creating a user profile as today, the actual creation of the user desktop is a matter of assigning the user to the appropriate pool or a new

virtual machine (also created in just a few clicks). Applications and privileges are determined by the group profile assigned, again with just a few mouse clicks.

Similarly, application testing is made more efficient as new virtual machines can be created virtually instantly. Delivery of applications would require clicking a checkbox; the user does not need to install software. By running all virtual machines on a server, no local data are stored, enhancing security for both internal and external devices. Hardware failures on the client side simply require a swap-out of the hardware…the user simply reconnects and they have their desktop back.

Delivery of new applications is significantly simplified when using virtualized applications. After IT tests and installs the new application, making it available to a profile is all that is required to deliver it. It will automatically be streamed to the desktop. As the desktop is composed dynamically, updates need to be done once to the base image and will be rolled out automatically to all users. As a result, there is no longer a need to update each device separately.

The use of virtual machines and virtual applications would provide detailed information on the number of users and the applications they use. While there are 3,739 applications currently deployed at USAID, usage information is not known. As applications are virtualized and updates centrally managed, it is expected that the number of applications will decrease.

Analysis

Implementing VDI and moving to cloud-based office productivity software, including email, is a high priority for USAID. While not all locations in which the agency has projects will have acceptable latency, or even connectivity, the agency feels strongly that improving access to IT resources, data, and collaboration in the field is vital to mission success.

Service Model

USAID will be obtaining IaaS resources to present their end users with a SaaS VDI solution and the associated infrastructure for identify management and authentication services..

IAAS will allow for capacity to be increased automatically based on resource demand. USAID administrators will no longer need to know or specify servers for the provisioning of additional desktops or users, and will only retain responsibility for the provisioning and decommissioning of users and profiles and for the installation of software required by the users.

From the business unit's perspective, the service model is that of SaaS. Desktops are quickly provisioned and de-provisioned based on end-user needs, and necessary applications made available within the virtual environment. End-users have no need to install, patch, or otherwise maintain their desktop environments.

Deployment Model

USAID considers a private cloud deployment most appropriate based on their assessment of risk and their technical analysis of VDI and the associated infrastructure for identify management and authentication services. The pilot is using the private cloud deployment model using existing data centers and hardware within USAID. It may eventually become a community cloud if USAID hosts VDI for other organizations, including other US government agencies or collaboration partners that work with USAID in fulfilling its core mission.

Cloud Computing Essential Characteristics

On-demand self-service

IAAS perspective: USAID service administrators can easily add more VMs from the cloud provider to increase server computing power as the demand for virtual desktop sessions or cloud-based applications increases.

SAAS Perspective: Virtual desktop are generated on demand. As an end-user's demands on a virtual desktop session increase, a greater amount of server resources are applied to the session.

Broad network access

Users will be able to access virtual desktops and applications use any type of client, including thick, thin, and zero clients, as well as mobile devices such as iPads, mobile phones, and PDAs.

Resource pooling

VDI enables increased sharing of computer resources. Traditional desktops have significant excess CPU and storage capacity, whereas tens or even hundreds of virtual desktops can be supported by a single VDI server, depending on the type of virtual desktop implementation.

Multi tenancy: different business units of USAID may be considered different tenants as currently desktops and applications for these units are distributed in many data centers or locations, many unknown to the USAID OCIO. When the same private cloud infrastructure is used to support other organizations in the State Department or other government agencies, these other agencies are tenants of the cloud.

Rapid elasticity

VDI provides a means for rapidly provisioning for both new users and applications.

Measured service

SAAS perspective: USAID OCIO is considering metered billing for the services it provides to its users. Virtualized desktops and applications would provide USAID detailed information on what services are being consumed and by whom.

IAAS perspective: the IAAS private cloud provider is expected to automatically control and manage its infrastructure to support USAID. The resource usage is expected to be monitored and reported with proper billing based on usage or other negotiated terms.

DRAFT

Security

The guiding principle followed by USAID in its security implementation is to secure and encrypt the data, and not the device. If the data are secure, the loss of a device does not compromise the data. As such, security must meet the FISMA data classification level of moderate, necessitating the use of two-factor authentication. For the second factor, USAID requires that RSA keys be used.

USAID intends to integrate their internet Single Sign-on (SSO) (e.g., Ping identity), second factor authentication (e.g., RSA SecurID), authentication and authorization credential repository (e.g., Active directory) with the VDI and their cloud-based applications. Their pilot has proved it is feasible.

By using a time-based random password as the second authentication factor and with the secure desktop profile generated on demand, USAID considers that the threat on accessing devices such as personal computers not a concern. For example, even if the computer is hacked and key strokes are recorded, the hacker won't be able to get into the VDI as the second factor is time dependent.

Cloud-based central maintenance and delivery of data eliminates data storage on portable devices. This is desirable given that privacy and data governance laws differ significantly between countries, and given the risk of lost or stolen mobile devices. Administrators should be able to control whether or not data are stored on local devices based on the device type (for example, iPad, laptop, or mobile phone).

Traffic is encrypted between the client device and the VDI in the cloud (e.g., citrix client on the client device and citrix server). Standard remote access authentication protocols must be supported. Finally, the host should log administrator actions.

Interoperability

For the VDI implementation, once a user is authenticated the first time, all of the applications within the workgroup are authenticated once the applications are integrated with the SSO solution. External applications, such as eTravel, web Time and Attendance applications, or HR applications, will require further integration. Web-based applications intended for use either as stand-alone remote applications or through the VDI will need to be integrated into the SSO solution. A standard for passing the security credential among identity management solution, second factor authentication, security credential repository and applications will be the key to facilitate the integration (such as OpenID).

Portability

The virtual desktop should be displayed with the same settings such as favorites, background, and software ("state / session persistence") on different access devices.

USAID has a well-controlled desktop environment with central data storage and access control credentials under Active Directory. Data migration is not expected to be an issue as existing files will remain on centrally managed file servers, although it is likely that users will need the ability to load files into a collaboration environment. Local directories on the PCs are for temporary use only and those data will not be migrated.

Users access a smorgasbord of 3,739 applications (each version of a product is considered a separate application). Only 7% (260) of all applications are installed on 99% of all machines suggesting that a base desktop implementation is definable. 1600 applications are installed on only a single machine.

USAID studied 45 applications in greater depth, each of which was installed on over 3,000 PCs, to determine how much work was required to virtualize those applications. It concluded that 12 applications were ready for virtualization, 18 may be able to be virtualized but further testing is required, 4 could not be virtualized, and 10 needed additional research before a determination could be made. Corporate applications should work seamlessly across virtual and traditional environments without necessitating a choice by the user.

The ability to virtualize, package, test, and deploy applications is a key element of the VDI solution. Since applications are not tied to the desktop OS any longer, easier, quicker, and more stable application upgrades should be possible.

Maintainability

The use of cloud and virtualized applications simplifies and speeds up user provisioning and de-provisioning. Applications and privileges are determined by the group profile assigned. Delivery of desktops and applications would become simpler: there is no longer the need to install software on user's workstations and it requires only the administrator to add the new app to the user's workgroups of their virtual desktop.

When provisioning new users, locale-based defaults such as workgroups and local printers, preferences, and settings should be inherited from the roles assigned to the user. During application and operating system upgrades and patches, user preferences and settings should be preserved in the same way as on a traditional desktop.

USAID believes that with virtual desktop solutions such as AppSense, the management of on demand virtual desktop can be achieved.

Usability

Desktop presentation should be the same regardless of what device is being used, unless a user specifically selects a native mode. Preferences should be persistent across devices. If a user is configured to access multiple desktops (for example, production, test, and UAT) then these environments should all be accessible on the same device, preferably at the same time with the ability to toggle between the environments.

DRAFT

Virtual desktop environments must provide a satisfactory end-user experience to users working with mobile devices.

USAID considers it is a must for users for users to rate the usability of the VDI solution as average or higher.

Performance

Network bandwidth may be an important factor for users to feel comfortable with the solution. For the project to be deemed successful, USAID expects that launching an application in the VDI environment will occur in no less than 90% of the time it takes on a standard desktop.

Resilience

Defined as the ability to reduce the magnitude and/or duration of disruptive events to critical infrastructure, the effectiveness of a resilient infrastructure or enterprise depends upon its ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event. Given the increased impact of a system outage to users relative to standard desktops (as discussed in Concerns and Challenges), rapid recovery from any outage is critical.

Concerns and Challenges

USAID identified five key metrics for user experience that must be met by a VDI implementation. First, users can continue to access and use data pertinent to their function. Second, they must rate the usability of the VDI solution as average or higher. Third, application launch in the VDI solution must occur in no less than 90% of the time it takes on a standard desktop. Fourth, users must award the performance of the VDI solution a rating of average or higher. Finally, users must be able to access the VDI solution from client devices on the internet.

USAID has determined that the overall FISMA data classification is moderate for its intended cloud applications. This necessitates a two-factor authentication solution that integrates with existing two-factor infrastructure. An additional factor is the fact that USAID has implemented an SSO solution, requiring that the VDI login request to receive a desktop also be integrated to submit credentials to other applications based on the user profile. This capability must be available from the time of VDI deployment as users currently have this ability.

Migration of 3,739 legacy applications could introduce significant complexity to a move to VDI. The initial target for migration is the 50 or so applications that are installed on 99% of the computers in the company. 1,600 applications are installed on but a single computer. Identifying what the appropriate solution is for each application will require significant effort. It is currently unknown what fraction of applications can be decommissioned and what fraction cannot be virtualized or web-enabled.

DRAFT

USAID users can be grouped by location: USAID Washington, USAID missions, and mobile users. The Washington locations are large facilities with high bandwidth and low latency networking and a large IT presence. Missions are geographic and functional offices that are connected to the central data center and have a small IT presence. With a few exceptions, latency is high at these locations. Finally, mobile includes employees connecting from non-corporate facilities. Bandwidth and latency are dependent on the country in which users are connecting.

These latency requirements affect the number of users who will be able to take advantage of VDI, and primarily affect the mission offices that generally lack bandwidth or have high latency. As a result, not all locations will be able to benefit from VDI, and mobile users will find those locations inhospitable to them. In some cases, local data centers could mitigate latency concerns.

A new risk arising from the use of cloud-based VDI is that an outage at the cloud-provider (whether on-site or hosted) affects all users. While risks such as this are present in specific applications such as email (if the Exchange server has an outage, email and calendaring is unavailable for all users), use of cloud-based VID creates a risk where there was none before. For example, if there is network problem or Microsoft Word is not working properly on one PC, other PC users can continue using Microsoft Word unaffected. Once the desktop is moved to the cloud, an outage can affect many users.

Data deletion is a significant challenge. For example, a user leaves USAID and their desktop is deleted. Is this deletion permanent, or does the desktop remain recoverable? Given successful deletion from system, there are likely to be backups with copies of the desktop. How can a cloud provider attest that all instances of old data have been deleted?

A major lesson learned by USAID during its pilot is that user training is extremely important. While VDI provides the same desktop, it is a challenge for users to use cloud-based applications or services with new user interfaces such as Google Mail or Google Docs.

This use case describe the scenarios that requires the on-site private cloud, outsourced community cloud, and the need for potential migration to an outsource private or community cloud. The issues and concerns common to these deployment models described below shall be addressed in greater detail by NIST SP 800-146.

For a private cloud to be reliable, the network must be reliable. Private clouds do not eliminate the requirement that the cloud subscriber organization have IT skills, although the skill mix may change. Private clouds need to be able to move workloads without the end users being aware. Workloads from different tenants may be running on the same hardware, separated only by security policies that, if flawed, may expose workloads between tenants. Network capacity may limit on-demand bulk data import/export and real-time or critical processing. On-site private clouds can have the same level of security as non-cloud resources. Finally, the on-site private

cloud could have a ceiling on resources available for computing and storage that would decrease elasticity.

Community clouds are also dependent on reliable networks. While workloads are hidden from clients, security perimeters restrict movement of workloads to the agreed-upon perimeter. Risks from multi-tenancy may increase the set of potential attackers due to the increased number of organizations. Data import/export and performance are dependent on network capacity between the provider and subscriber. Similar to a private cloud, security perimeters can be hardened, although both the provider and subscriber perimeters need to be created. Unlike an on-site private cloud, providers are more likely to be able to provision a large cloud as needed, although elasticity is possible only with a large enough cloud with heterogeneous workloads.

DRAFT