mess-kit wiki-doc

Main Page

From Wiki

Welcome to the MESS-KIT wiki: **Minimum Essential Software Services for Knowledge and Information Transfer**

- Introduction to the MESS-KIT -- The philosophy, design and construction of the MESS-KIT
- A History of the MESS-KIT -- How it all got started, an insight into the philosophy and design
- Guide to using the MESS-KIT in the field -- Hands-on instructions for use
- Best Practices -- Tips and tricks on how to make the system work better
- Troubleshooting -- What to do when you don't follow the Best Practices
- Demo -- What I'm going to do for my demo this week
- Users -- What skills are needed to use the MESS-KIT

II. Structure
The MESS-KIT system is composed of three basic components -- the software package, the virtual environment and the hardware:
a. APPLICATION SOFTWARE PACKAGE: One or more Virtual Machine Instances that package together an operating system with a web server environment and all free-and-open-source/commercial-off-the-shelf software modules. Example: A VMware instance of an Ubuntu Linux installation with a full LAMP web server hosting environment and associated web software.
b. VIRTUAL MACHINE CLIENT SOFTWARE: One Virtual Machine Software Client to package, distribute, and host one or more Application Software Packages and abstract the application software from the host operating system. Examples: VMWare Fusion and Sun VirtualBox.
c. HARDWARE: Hardware on which the Virtual Machine Client Software and Application Software Package will run. The Hardware will include a host operating system. Examples: MacMini running OSX, ASUS eeePC Netbook running eeeBuntu Linux.

III. More information
Click below for a sustained analysis and explanation of the MESS-KIT system:
a. Conceptual Framework
b. Operational Concept
c. Architecture and Organizational Design
d. Technical and human performance
e. Information Assurance
f. Support and Training

IV. Manuals and Documentation
Click below for step-by-step instructions for numerous MESS-KIT functions:
a. Installation Guide: A guide to setting up the tools necessary to operate a MESS-KIT.
b. Software Guide: A user guide to running various MESS-KIT software packages.
c. FAQ Page: Answers to common user questions.
d. Technical Documentation: Various technical documents relating to the project.

[edit] Getting started

- Configuration settings list

- MediaWiki FAQ
- MediaWiki release mailing list
- Consult the User's Guide for information on using the wiki software.

Introduction to the MESS-KIT

From Wiki

Jump to: navigation, search
Introduction to the MESS-KIT
In-short:
The MESS-KIT is an attempt to make it easier to do a rapid IT deployment. When disaster strikes, those heading into the field often do not know what they will be facing when they get there, and there's no internet for phoning home. The goal is to provide the tools necessary for quickly and flexibly standing up the tools necessary to run a project out in the field with minimal infrastructure.
Why? Read a little about the History of the MESS-KIT
How? Read the Guide to using the MESS-KIT in the field

A longer explanation:
The MESS-KIT system will improve the ability for partners of stability operations to share unclassified information about reconstruction activities. Focusing on non-governmental organizations (NGOs), private volunteer organizations (PVOs), local NGOs, local governments, provincial reconstruction teams (PRTs), agricultural development teams (ADTs), human terrain teams (HTTs), and other partners to stability operations, the MESS-KIT system will provide for a wide variety of data and information to be shared. In addition to sophisticated imagery and real-time information, the kit allows for partners and actors to share the information generated during normal operations. Information about best practices, updates on projects and operations, as well as reservoirs of cultural expertise will add to the data set the military focuses more specifically on acquiring. This type of information can prove to be extremely valuable to actors in the field, greatly enhancing project success.
This kit will focus on radical simplicity of design, encapsulating complexity wherever possible within modules of either Free and Open Source Software (FOSS) or Commercial, Off-the-Shelf (COTS) software. It will also harness social networks that already exist within and between organizations to accelerate adoption of the platform and to catalyze information exchange.
The MESS-KIT allows for a number of interrelationships and communications. When deployed to an organization, the organization will have the ability to network and collaborate with USG departments and agencies, UN, and other NGOs, as appropriate, linking up efforts. In other instances, connecting an individual, in particular if that individual is a “super-connector” with a dense social network, the impact of providing connectivity tools to that individual will be great. The structure of the MESS-KIT means that any number of relations – between individuals, organizations, internationals, and locals, are possible, and they can be tailored to each situation as appropriate.
Each kit provides the partner with a core suite of software and hardware tools that can store, process, and exchange unclassified data via XML (Extensible Markup Language) feeds. In cases where a partner has weak information communication technologies, the MESS-KIT bridges the digital divide, allowing the partner organization to participate in existing coordination mechanisms, share and access information, and identify opportunities for collaboration.
Restoring a country to stability and placing it on the road to partnership in the community of nations is a systems problem, requiring coordinated action between hundreds of organizations. The vision of the MESS-KIT is a first step towards a larger

information sharing strategy that will foment information sharing between these organizations, with the vision of increasing the tempo and volume of communications between them, improving coordinated action, and eventually reducing the time and resources necessary for successful completion of a CMO operation.
Unlike military information communication technologies, the MESS-KIT fosters *radical inclusion.* There is an old adage in network theory: one fax machine is useless; it requires at least two to be worth anything. In the same vein, the practical value of networks increases with each new user. From cell phones to the Internet, the utility of the communications network is a function of the number of users. And because each new user adds not just one new link but many possible new relationships, the growth in the utility of the network increases at an exponential rate.
Retrieved from "http://192.168.1.50/index.php/Introduction_to_the_MESS-KIT"

Conceptual Framework

From Wiki

Jump to: navigation, search
The MESS-KIT is the result of pragmatism rather than theory. It was born of the 'lessons learned' and hard-earned field wisdom from recent projects, including counter-insurgency (COIN), security, stability, security, and reconstruction (SSTR), and humanitarian assistance/disaster response (HADR) operations in Haiti, Iraq, and Afghanistan, as well as the 2004 Indian Ocean tsunami, the 2005 Gulf-Coast hurricanes (Katrina and Rita), and earlier engagements in Bosnia and Kosovo.
The MESS-KIT draws on the following combined experiences and ideas:
Alignment of civilian, military, and local efforts is a *requirement* for effective operations.
Civil society requires the alignment of a vast array of assets and people. As such, it is most effectively achieved through a robust and densely interconnected network of coordinating partners. When CMO (Civil Military Operation) partners act in a coordinated fashion, they can dramatically reduce the resources necessary for the achievement of the mission. When they act in an uncoordinated fashion, they undermine one another's efforts and waste assets in already resource-constrained environment. They also can cause additional damage. As discovered multiple times in several cultures, the impact of too many disconnected efforts can be quite dramatic. Incoherent and redundant activities may undermine local faith in the international response and may make cooperation between CMO partners even more difficult as the projects wear on. These negative feedback loops, in turn, may demand a further increase in resources to accomplish objectives, and may grow so resource hungry as to eventually inhibit or prevent mission success. This detrimental result should be avoided at all costs.
Communication is a necessary precondition for coordination and cooperation.
Complex projects tend to be dynamic: after a major shock to an affected nation,, for instance, military and civilian organizations scale their participation over time. During this ramping up, information-sharing problems can quickly create coordination problems: as more donors and projects emerge, the need for coordination increases quickly. However, communication between organizations rarely keeps pace with the desired level of coordination. More commonly, information shared between stability partners diminishes over time. This focus on protecting information usually leads to conflicts and an accompanying breakdown in trust between the independent actors. Thus begins a vicious cycle: as trust decreases, the amount of information flowing between partners decreases. This leads to further breakdown in coordination, more conflict, and ultimately, decreasing levels of trust and reduced information sharing. These challenges factor heavily in the dissolution of cooperation and the opening for insurgent activities after a disaster or conflict. When trust dissipates between CMO partners, information sharing gets limited to carefully prescribed reports and ground truth gets lost to all but those

who are closest to the affected population (who may well be insurgents, actually). Through the degradation of trust and coordination, the security of CMOs can greatly diminish, too, making civilian operations far more risky, costly, and ultimately, less effective.

Open and proactive communication between partners is the antidote to this downward spiral. In operations where civilian and military goals differ considerably (as in cases of violent conflict or direct military action), communications can help partners get along effectively without attempting to align objectives or seek out opportunities for collaboration. In other instances, when the goals of civilian and military actors may be closely aligned, communications might span the gamut—from a minimum level of cooperation to a robust cooperative collaboration. In either case, communication serves as a catalyst and enabler to other activities. A shared understanding between all the partners regarding the area of operation and human terrain is a needed for productive discussions about strategy and operational approach. Only through a common operational picture and a shared set of objectives will partners reconcile those differences and develop a plan towards unity of effort. After all, that is the goal.

Partners begin with different conceptions of how to work together.

The leaders of multinational CMOs cannot assume that all parties will be using the same methods for thinking through strategy, tactics, or operations. Any technologies brought to the table will likely reflect the approach of the partner (or vendor) who funded or produced their information and communication technology framework. Sectors have often developed sophisticated coordination mechanisms that are unique to each field. In some operations, the UN Office of the Coordinator for Humanitarian Affairs (UNOCHA) has the lead, whereas in other cases, local governments may lead any international intervention effort. The protocols, standards, and data schemas—as well as the styles and etiquette—differ considerably. An awareness of and sensitivity to these differing technical and social norms is crucial for the success of any effort.

Informal networks are the mechanism for finding common ground

As is normally the case, agreements between partners are often not made through formal command-and-control structures with clear mechanisms for accountability. Instead, these agreements are made through information networks. These informal arrangements in the field are often the best (or only) mechanism for aligning efforts between local nations, NGOs, IGOs, and other entities. These improvised arrangements don’t just occur between leaders; they can occur at all levels of the partnering organizations. It could be junior members of several organizations—local or international—who have access to the combination of actionable information and local relationships necessary to turn that knowledge into a constructive outcome.

Technology that enables informal networks also needs to enable improvisation

Earthquake operations will require tracking people entrapped in collapsed buildings, for instance. Other operations may deal with disease outbreaks or insurgencies. In each case, the informal networks will improvise ways to handle these issues, and their ICTs must be flexible enough to enable the informal and formal exchange of information within the negotiated frameworks—the structure of which often cannot be anticipated by the creators of the information and communication technologies. As a result, technologies (and technologists!) on each side of the divide must be mashable enough to allow interoperable communications to emerge over time.

Blanketing the operations with communications accelerates coordination

Field operations have not yet developed a standard operating procedure to harness the desirable effects of blanketing an area with communications that all partners to a CMO can access. This is a huge problem. Normally each organization tends to shell out tens of thousands of dollars for the backhaul costs of satellite communications. As a result, these organizations tend to limit the access of outsiders to their networks. This restriction on packet flow corresponds directly with a reduction in information flow. And that’s not good at all. The situation also forces each organization to build its own hub and spokes network—an often unnecessary redundancy in austere settings where the use of every resource must be optimized. Blanketing the area with open communications networks—from TCP/IP (Transmission Control Protocol/Internet Protocol) to SMS (Short

Message Service) and cellular voice services—removes this obstacle and is less costly than trying to fix an uncoordinated response.

Partners without flexible ICTs should be given adequate tools, right?

Because so many of the civilian partners to CMOs lack effective, adequate, or up-to-date ICTs, interoperability with other partners cannot occur until these organizations possess some ICTs to connect into the communications network. Now, in this case, it is the interest of ALL partners to the CMO to ensure that organizations without modern ICTs should be granted some set of *minimum essential software* and services to enable information flow about issues of importance to the overall operation.

Most information generated at the field level can be shared with all CMO partners. So, why is it not?!

While the mantra of "hold information private until made public" has its place for operational security of kinetic activities, most information pertaining to operations for disaster response, stabilization, transition and reconstruction can be shared with CMO partners (and should be). In the case of recent operations, the United States Government has unnecessarily over-classified vital information—either as LIMDIS (Limited Distribution), FOUO (For Official Use Only) and/or NOFORN (Not Releasable to Foreign Nationals/Governments/Non-US Citizens), and has thereby impeded cooperation with the United Nations and other international NGOs. Instead of mitigating risk, this act of closing off information channels increased the risks borne by both responding organizations and the affected population. Conventional OPSEC (Operations Security) wisdom defaults to over-classification. But the United States Government, from 9/11 onwards, has recognized the importance of a "need to share" rather than a "need to know" paradigm. It must be stressed that NGOs and IGOs have their own problems that they must resolve as well. But, this is how the MESS-KIT system can inform and improve—through facilitating cooperation between civilian and military partners by providing a communication infrastructure for NGO and IGO communities.

Technology and policy should remove extra steps for sharing information. But, they don't.

Current procedures to do not adequately calculate the risk of not sharing information. Instead procedures only focus on the possible negative consequences of its release. This risk analysis needs to incorporate the impact of keeping too much information "close hold," which may entail CMO mission failure. What is rarely recognized is that the opportunity costs of withholding information may often outweigh the potential risks of sharing that same information.

Technology should recognize the difficulties of communications in austere environments.

While Web-based tools may look nice in the office, slow connections in the field may render even the best-designed web site unusable. Worse, intermittent connections require tools that support disconnected use. Many technologies that are familiar are unsuitable in these contexts without great modification.

Operational Concept

From Wiki

Jump to: navigation, search

MISSION

The MESS-KIT augments the capacity of civilian-military project partners to work together by enabling three distinct things:

1. Information exchange within single civilian organizations
2. Information exchange between multiple civilian and military organizations
3. Strategic communication with the area of operation.

1. Information exchange within civilian partner organizations
Many partners do not posses ICT (Information Communication Technology) frameworks that allow for rapid exchange of tactical information within their own organizations. The MESS-KIT—as a standalone unit or as a system of linked units—can provide these civilian partners with basic ICTs to enable them to coordinate their own activities.
2. Information exchange between CMO partner organizations
Interoperable ICTs between civilian partners are not always available. But that's okay. Some partners are using state-of-the-art software packages with XML (Extensible Markup Language)-based web services. Others use email as the primary means of exchanging documents and data sets, or web portals with overstuffed directories of files and blogs. Some use paper or bridge the digital divide by deploying human messengers with USB memory sticks or floppy disks transferred between sites (which is known, informally, as "sneakernet"). The MESS-KIT provides a common platform for civilian organizations to exchange data, track the progress of projects, and create conferences and discussions between personnel involved in projects in similar sectors.
3. Strategic Communication
Successful COIN (Counter Insurgency), SSTR (Stability, Security, Transition, and Reconstruction), and HADR (Humanitarian Assistance Disaster Relief) operations incorporate local perceptions and attitudes into all aspects of analysis, planning, execution, and assessment. They create a feedback loop between activities in CMOs and the "perception effects" arising in response to these activities. These efforts, called "strategic communication" (SC), help partners share each other's knowledge and resources to achieve project objectives. Through this work, all partners gain a richer understanding of the local populations perceptions and needs. The better informed the CMO partnership is about the context in each of these settings, the more effectively can they tailor activities to accomplish the stated goals.
VISION
Restoring a country to stability and placing it on the road to partnership in the community of nations is a systems problem (and a large one at that!). It requires coordinated action between hundreds of organizations. The vision of the MESS-KIT is a first step towards a larger information sharing strategy that will encourage information sharing between these organizations, with the vision of 1) increasing the tempo and volume of communications between them, 2) improving coordinated action, and eventually 3) reducing the time and resources necessary for successful completion of a CMO operation/project/mission.
GOALS AND OBJECTIVES
• Create a shared platform for exchanging and updating essential information between CMO partners, including maps, imagery, photography, videos, documents, and data-sets.
• Provide relevant and useful content (localized to the AO (Area of Operation)) to CMO partners, thereby also seeding the AO with important ideas and data.
• Increase volume and tempo of communications between CMO partners, enabling them to spot problems earlier and to reduce delays in the system.
• Enable deeper and more sustainable informal networks among CMO partners.
• Create a useful leave-behind for host-nation ministries and other partners who will be working in the AO for the long term.
SYSTEMS CORE FUNCTIONS
A MESS-KIT consists of five basic elements:
Hardware: A mini-server with attached storage and networking to support up to 12 people. NB: Server hardware is not a required component of the as-supplied system, aside from the memory device on which the MESS-KIT is loaded; however it is specified here for explanatory simplicity. Hardware can be supplied which conforms to minimum standards.
Software: A suite of configurable applications to provide minimum essential services for a single CMO partner and to provide for the exchange of data between partners.
Individuals: The fields staff of CMO partners who have access to a MESS-KIT.

Relationships: The existing relationships between the field staff of CMO partners as well as the relationships build as a result of sharing information via the MESS-kit.
Activity Streams: A flow of events carried out by individuals working through the informal network (relationships) that bind together CMO partners. The deployment of a MESS-KIT involves two components: the provision of one or more technology platforms (hardware and software); and a set of practices to develop relationships between multiple individuals with the intent of mobilizing them to coordinate actions across multiple organizations. Activity Streams are not a component of the system so much as signals sent between partners about the status of their actions. They can be as simple as a short text message (SMS) or a complex document with many attachments and diagrams.

OPERATIONAL CONCEPT

From the perspective of civilian partners, the informal networks by which most coordination of effort occurs rarely possess the needed ICT frameworks to support either the operational tempo of military forces or the demands being placed on partners by the complex coalitions in which they are asked to work. Poor communications over incompatible ICTs becomes an insufficient coordination mechanism when the operational tempo of the CMO exceeds the mental bandwidth of the CMO partners. Where paper and unreliable cell phones are the primary means of communication, this bandwidth limit may be reached almost immediately.

When CMO partners fail to have close communications and operate without unity of effort, they open opportunities for insurgents and other elements to disrupt operations, degrade mission effectiveness, and push back the timeline for the strategic vision set by the international CMO partnership. This situation will only worsen as insurgents make more sophisticated use of social media tools currently being used by activists in authoritarian states. What is particularly troubling is that military and civilian partners to CMOs generally lack tools to mobilize the collective experience and intelligence of the host nation's populace, even while tools like SMS text messages are showing the power of bottom-up organizing in the developing world. The failure to share information between CMO partners creates high and often unacceptable opportunity costs in a resource-scarce and time-constrained environment.

The MESS-KIT augments the capacity of CMO partners to communicate and coordinate their activities. It provides a set of Minimum Essential Software and Services for basic field operations and information operations. It operates at three levels: 1) building the capacity of a civilian partner; 2) fostering coordinated actions among several civilian partners; and 3) enabling effective information operations and strategic communications efforts.

1. Building the capacity of a local partner

Many civilian partners possess a slew of ICTs from several eras of computing, many of which are incompatible with each other or which have been cobbled together from spare parts. Some still rely on paper-based systems (as is the case with many district and village offices of host-nation ministries, NGOs, and local contractors). If these partners are going to be integrated into coordinated operations, they first will need a shared set of low-cost ICTs which can be maintained and extended using local labor. The MESS-KIT provides a low-cost set of hardware and software that the military can grant to one or more local civilian partners, providing them with the basic tools necessary to coordinate action within their own offices.

The MESS-KIT also provides a critical tool for recruiting civilian partners who may not initially trust the military. Because the configuration of the MESS-KIT is flexible, it can be preloaded with key data about the area of operation, including recent aerial imagery, maps, and human terrain, such as key political players, local chiefs, or other important persons. Within the informal networks in the field, recent aerial imagery is one of the most valuable currencies. Because the demand for the MESS-KIT is a field-driven initiative, many aspects of its deployment would be left to the ingenuity of the local commander, PRT (Provincial Reconstruction Team), ADT (Application Development Tool), HTT (Human Terrain Team), or civil affairs unit. A MESS-KIT would likely be deployed in the following manner to individual partners:

Conceptual Scenario 1:MESS-kit in standalone mode

A PVO (Private Voluntary Organization) enters a region and discovers that a local national has organized an NGO to foster cross-ethnic dialogue. She operates from a community center with six staff members and has developed a community of 200 women to participate in afternoon programming. The women bring their daughters, and the NGO is considering expanding the program to teenage girls. The center has recently lost its one aging computer, which it used purely to track member participation and accounting. Otherwise, it operates purely on paper, cell phones, and SMS. The PVO would like to integrate the NGO into a larger program to foster education for women, focusing on retaining teenage girls in school. The PVO gives the NGO a MESS-KIT plus six low-cost "Netbook" computers, and contracts a local national to educate the NGO's staff members on the use of word processors, a web-based database of students, and a web-based tool for managing SMS groups.

2. Fostering coordinated activities between several civilian partners

If a commander encounters a situation in which multiple partners require basic ICTs, and/or if CMO partners cannot devise a mechanism for interoperable ICTs, two or more MESS-KITs can be distributed to CMO partners. This distribution model creates MESS-KITs which cross-subscribe to data feeds from one or more of its included applications (in most cases, subscriptions will be made to the document management application, blog, wiki, and disaster management system). This mechanism creates the basic building blocks for wiring the informal networks of a CMO. This distribution mechanism would likely not follow a top-down directive to distribute MESS-KITs to every partner simultaneously. Rather, it would scale from the bottom-up, based on the identification of important partners by individual PVOs or PRTs, ADTs, HTTs, and other civil affairs teams. A typical deployment might look like the following conceptual scenario:

Conceptual Scenario 2: Hospital and Local Health NGO

A PVO (Private Voluntary Organization) begins working with local hospital on a youth vaccination program and a local NGO that is also working on youth health programs. The hospital has no computers to devote to the effort, and the international NGO is using a Windows 95 machine that has been cobbled together from spare parts! It is buggy and the computer is infected with multiple viruses. The PVO issues MESS-KITs to a local hospital pediatrician who is managing vaccinations and the program manager for the NGO. The PVO works with MIT's FabLab on contracting local nationals to create WiFi shots between the NGO and the hospital, using open-source tools, and to encrypt the network with WEP (Wired Equivalent Privacy). The PVO works with each side to show the pediatrician and program manager how to subscribe to each other's RSS feeds, creating several cross subscriptions:

1. A feed from the hospital's HIPAA (Health Insurance Portability and Accountability Act) compliant patient tracking system, which releases aggregate demographic information about how many youths have been vaccinated during the week, including shape files of the areas in which vaccinations have occurred.
2. A feed from the NGOs public health database which shows the areas in which field workers have been going house to house to convince families to vaccinate their children.

Together, the hospital and the NGO are able to see the direct results of vaccination outreach program. Similarly, the NGO is better able to convince its donors to fund additional work with actual aggregate clinical data.

3. Technology for Bureaucracy v. Technology for Informal Networks

Technology is frequently modeled on the inflexible structures of the bureaucracies that funded its development and gets in the way of tools that enable informal networks in the field. These technologies are poorly suited for the rapidly changing environments characterizing conflict, post-conflict, and disaster response scenarios. Inflexible policies around technology often leads to a vicious downward spiral: diminished communications cause a breakdown in the informal networks, which makes the necessary trust on which unity of effort depends also break down. It is common to observe partners to COIN, SSTR, and HADR operations engaging in the following dynamic: to ensure operational security or prevent the military from accessing civilian data, partners to COIN, SSTR, and HADR operations hold back information critical to ensuring ongoing consensus. This action signals diminished trust and leads to uncoordinated actions, which in turn drives

more distrust and diminishes the overall security environment, not just the information security situation.

4. Obstacles to Field Fixes to Inflexible Technologies

In order to provide workarounds for blockages presented by inflexible technologies, personnel from partnering organizations sometimes must resort to inefficient and ineffective measures. Common blocks in the flow of information between partners include:

• *Closed Networks.* Many information assurance architectures are designed to prevent access by outside parties through limiting access to the transport mechanism: the network. One of the architectural legacies of this design choice is an inability to grant access to these ICT resources to external partners, because access to these resources would first require credentialing those partners as internal members of the host organization.

• *Unnecessary Classifications.* Many documents are over-classified with For *Official Use Only*, *Limited Distribution*, or *No Foreigners.* In the case of private organizations, many are marked Confidential or Privileged. In most cases, information on these documents can and should be shared at the field level with partners, but must be withheld to abide by organizational policies and governing laws.

• *Unnecessary Permissions.* Many software applications specify their default security settings for each document to make that information available only to the creator or the creator's immediate work group. Overburdened field staff tend not to change this setting, leaving a great wealth of otherwise public information stuck on individual hard drives.

• *Firewall Blocks.* In an effort to prevent access to unauthorized information, firewall blocks can prevent whole blocks of domain names from being accessed. In one case, a military unit responsible for monitoring Afghanistan's government web sites for reconstruction projects were blocked from accessing all sites ending in .af, which is the top-level domain for Afghanistan.

• *Opaque Data Schema.* Many data formats are proprietary and require the purchase of expensive software to convert them to open data format that partners can use. This cost in time and software licensing often prevents data from being shared.

These issues frequently cause problems:

Inflexible Homegrown Workarounds: While elegant mashups do occur in the field, more frequently, personnel are under time and resource constraints and deploy a solution which matches the need at the time it was created and which does not elegantly scale to meet changing needs.

Duplicate Data Entry: In cases where information exchange between incompatible systems is critical, personnel from two or more partner organizations may choose to manually import data from one system to another—sometimes by hand. Repeat data entry is inefficient, ineffective, and unsustainable. Agreements to perform duplicate data entry will diminish in effectiveness over time and/or during crises (which is when shared information is most needed). It should be noted that partners will often refuse to perform duplicate data entry into .mil-based systems solely for the sake of unity of effort.

5. Working in an inefficient and often ineffective system for international development and reconstruction

The numerous actors in conflict, post-conflict and emergency settings have contrasting—and often competing—objectives. Military commanders face another challenge in finding opportunities for collaboration between civilian partners: the international development system is neither optimally organized for creating synergies between partnering organizations nor designed to foster coherent, fast action. In many cases, NGOs compete among the same donor pool for grants. The sub-agencies of large IGOs may have agendas that make interoperability more difficult than would normally be assumed. The military must learn to differentiate factions among non-governmental entities. Humanitarian NGOs have different agendas than NGOs focused on the eradication of a single disease, the provision of clean water or renewable energy. Likewise, religious NGOs may have cultural agendas that can clash with the agenda of other organizations —particularly those NGOs which focus on reproductive health.

Architecture and Organizational Design

From Wiki

Jump to: navigation, search
Technology does not create unity of effort by itself; networks of coordinated teams do. An information sharing system requires a network of supporting individuals at its endpoints, working with one or more enabling technologies. The MESS-KIT offers an enabling technology within a set of tactics, techniques, and procedures (TTPs) to augment the ability to coordinate activity across a CMO. It is divided into two segments: 1) an enabling technology platform and 2) a set of practices to generate information sharing activity between CMO partners.

1. Enabling Technology Platform

The MESS-KIT consists of a system of bundled technologies, drawn from both the open source and commercial worlds. These software tools are configurable to the AO (Area of Operation) and may add additional toolsets as it is deemed necessary and appropriate. The core toolset includes the following elements:

a. Hardware Platform Specification

The hardware specification recommends a small server to enable the operations of a workgroup no greater than 12 people. The hardware recommendation consists of six components:

1. Mini-server
2. Network router
3. External Storage Device
4. Storage Case
5. Uninterruptible Power Supply
6. Cabling

NB: The server should not be used as a workstation; to do so may potentially compromise system stability. The server can be configured for use as a workstation in case of inadequate hardware for all users, in which case, it should be carefully monitored by the administrator.

Optional. In some configurations, it may be desirable to include inexpensive "Netbook" computers with the server, especially in circumstances where CMO partners have outdated PCs or no PCs at all.

b. Software Toolset

The MESS-KIT includes a set of basic collaboration software appropriate for the field. The core tools include:

1. Document Management System. Ex: Knowledge Tree.
2. Survey Management System. Ex: Lime Survey.
3. Disaster Management System. Ex: Sahana.
4. Online Meeting Software (VOIP and chat). Ex: DimDim.
5. Wiki. Ex: MediaWiki.
6. Blog. Ex: WordPress.
7. Photo Gallery. Ex: Gallery.
8. Course Management System. Ex: Moodle.
9. Content Management System. Ex: Drupal.

Optional configurations include:

1. Raster Aerial Imagery Browser: A simplified web-based GIS application. Ex: Google Earth Enterprise Browser.
2. Georeferenced Data Visualization Software: a tool to enable advanced development and visualization of geo-referenced datasets on aerial imagery and/or maps. Ex: GeoCommons.

2. Information Sharing Practices

The MESS-KIT relies on a set of TTPs (Time Triggered Protocols) around effective information sharing, developed and refined over the past ten years in Iraq, Afghanistan, Banda Aceh, and other SSTR, COIN, and HADR operations. These information sharing practices focus on the development of relationships between individuals who participate in civilian-military operations, as well as formal frameworks between the participating organizations. The core ideas include the following insights:

Wire the informal networks: Because the informal networks are the key to operating under "Hand Shake Con" and because these networks are rarely enabled by interoperable ICTs or reliable bandwidth, those units who are deploying MESS-KITs should grant these tools to the partners who compose the informal networks of the CMO. MESS-KITs can connect to each other via simple local WiFi networks, or even sneakernet.

Connect the Superconnectors: To speed adoption within the informal networks, it is often best to identify the most likely champions: the superconnectors, the individuals who are the hubs on the social networks who can provide entry into closed networks and who can bridge sectors. These individuals are often the most willing to try new communications tools that can save them time and help their "people" to build a more effective response.

Be radically inclusive: Military ICTs tend to operate under strong information assurance mindset that seeks to exclude everyone except those specifically authorized to view atomized bits of information. This is rarely a helpful model. Instead, the MESS-KIT fosters radical inclusion. There is an old adage in network theory: *one fax machine is useless; it requires at least two to be worth anything.* In the same vein, the practical value of networks increases with each new user. From cell phones to the Internet, the utility of the communications network is a function of the number of users. And because each new user adds not just one new link but many possible new relationships, the growth in the utility of the network increases at an exponential rate with each new user. This allows for the catalytic effects needed to make an impact in challenging environments. There is no question that including everyone in an information sharing system is difficult. This dynamic must start small, within a controlled environment and only then "scale outward." That said, it should include all voices, including and especially those who traditionally have been left out of governance (lest they begin again the cycle of violence). This level of inclusion shifts the information-sharing paradigm, from one which hides information lest it be discovered and utilized for strategic ends, to one which undermining threats by raising the level of visibility of all activities, following an adage from United States Coast Guard ADM Thad Allen, "transparency generates self-correcting behavior."

Keep technology simple, mashable, and flexible:

As technologies whose complete functionality has been determined in advance by a team of cubicle-based engineers are brittle, when confronted with the need to adapt to changed requirements and adaptations necessary under COIN and SSTR projects, these technologies break. Tools designed for fast-changing projects must accommodate the inclusion of partners whose participation was never imagined. This is essential. These tools must therefore be sufficiently simple for everyone to understand; mashable in ways that enable cross-application data flows that can be designed to meet changing needs; and flexible in their application to new problem domains.

Develop common, open data schema:

The use of common data schema are a key element of information sharing. Because each organization brings its own traditions and models to CMOs (Civil Military Operations) , they also bring their own naming structures (taxonomies) and concepts of operations to the theatre; they tend to embed these concepts into their data structures. Reconciling these issues is not only technical; it is also political. It requires creating mapping of concepts, which can become contentious. Resolving these differences, however, is the key to effective communication. If everyone can describe the same phenomenon using the same language, efficient operation becomes a possibility.

Provide Systems as a Service to Partners:

Collaboration techniques that duplicate efforts and require double data entry fail due to time constraints in the field. Providing resource constrained partners with systems that provide useful services (maps, imagery, document management, etc) will enable people to perform essential tasks in an easier way.

Remove extra steps for sharing information:

When busy field staff must make active additional efforts to share information, the expected result is that no information sharing will take place beyond that which is essential to the tasks at hand. This minimum level of information sharing regularly overlooks important opportunities to collaborate and coordinate and often results in conflicts and other miscommunications. Technologists and managers should endeavor to make information sharing the default position of all processes and applications.

Entrust partners with information about non-kinetic operations:

Operational security will prevent release of warnings about many kinetic operations. However, most information about non-kinetic operations—especially about reconstruction and development activities—can be made public to partners. Over classification of documents should be consistently discouraged.

Learn from operations and adapt the MESS-KIT to actual needs:

The informal networks inherent to the fast paced and ever changing HADR and SSTR projects can help evolve the information sharing system based on real lessons learned in the field. They should also amplify the growing capacity of the system's users to alter the tools to meet their own requirements, as this capacity to create tools is a core element of making a society self-sufficient in the long term.

Technical and human performance

From Wiki

Jump to: navigation, search

EXPECTATIONS

The MESS-KIT system augments the capacity to generate unity of effort; it does not guarantee unity of effort. The success of the system will in large part be dictated by the efforts of humans using information sharing technology across the boundaries of specific organizations.

Technical Expectations

The MESS-KIT uses both commercial off-the-shelf (COTS) and free and open source (FOSS) software, hardware, and services which are available under FOSS or commercial license and are not subject to U.S. export restrictions. It also relies on the public Internet for communications. Where possible, the MESS-KIT recommends the use of WEP encryption for uses over WiFi networks. All products implemented must be releasable to the coalition countries and must inter-operate with the commercially available products and standards found in the USA and each country; they must also be compatible with the coalition partners' communication infrastructure to ensure all countries can access the network.

Data Synchronization

The data mesh connecting the various devices is scalable, but it is not 'n-scalable.' Each kit will support 12 users and will be able to cross-subscribe to XML (Extensible Markup Language) data feeds with many other kits. Cross subscription of feeds is often limited by the ability of individuals to process the resulting volume of information flows and by the memory space on the device; this cognitive limit—combined with a strong incentive to keep open drive space—will effectively prevent scaling beyond the technical capacities of the system. No limits will be placed on cross-subscription aside from training of users to understand their own information processing limits. Scaling of the system needs to be

actively monitored. Methods for allowing for some organizational designs other than a pure mesh will likely need to be explored. Conflicts between computers which have been operating in standalone and disconnected use may require manual intervention, though version control is not part of XML/RSS feeds and will not therefore require substantial conflict resolution.

Data Storage

Systems which have been operating for long periods may fill their default hard drives without human intervention. Periodic archiving procedures for moving old files to backup drives thus freeing up space for new activities is recommended. This procedure is no different that the care of a personal laptop, which requires a similar process.

Database and File Size

It is recommended that no single database size exceed the available RAM or the file size of 4GB. It is also recommended that no single file exceed 4GB in size or the size of available RAM.

Human Expectations

The issuing of authentication credentials to individual users also recommended. Activities by individual users should be monitored by their effects on the informal agreements that govern CMO partner interactions. Reputation-based management systems may be incorporated in the future based on field experiences with the device.

SYSTEM PERFORMANCE

Metrics

Measuring the effects of information sharing is a traditionally difficult endeavor. Many effects have long delays between the transmission of a single meme and its application to one or more operations. Some memes cannot be disaggregated from contextual information which is unique to the perspective of an individual user, or from a web of actions around it. Over time, the effects of tacit knowledge and accumulated cultural wisdom are difficult to calculate. That being said, the feedback loops that govern information flows are very important to monitor. When information flowing into an organization dwarfs the information flowing back out of that organization, partners in CMO will reduce the information that they give to what is perceived to be an "information sink." If they are going to continue to contribute, partners need to receive some value in exchange for sharing. They also respond strongly when the information supplied to a partner is seen to result in visible action.

Standalone Measures of Performance

Most performance measures for individual MESS-KITs relate to the usage of the device. Metrics may include:

1. Total files uploaded by all users
2. Total files accessed by all users
3. File contribution rate per user
4. File access rate per user
5. Total searches for files
6. Total wiki and map entries created
7. Total wiki and map entries updates
8. Total blog posts created
9. Total blog posts viewed
10. Total hyperlinks created between files on the system and entries in the wikis, maps, blogs, and other database-backed entries on the system.

Information Assurance

From Wiki

Because the MESS-KIT system enables the informal networks to share information across organizations and nationalities, the dictates of information assurance raise challenges. Several principles must be followed:
1. *Unclassified Information Only:* The MESS-KIT is designed to carry unclassified information between partners. Any information with classification must pass between partners via other channels.
2. *No Personal Information:* In addition, the MESS-KIT is not intended to store personal information, and is not intended for applications which require HIPAA-compliance or which must conform to personal data privacy standards in the United States, European Union, or other countries with analogous regulations.
3. *Use of commercial best practices:* The system will use commercial practice of having login accounts for individual users and assuming basic WEP encryption of the network (in cases where WiFi is used). The system will not use IA practices for military systems, as it is these practices which are contributing to the lack of information flow between the DoD and non-DoD partners.
4. *Protection of Activists:* The MESS-KIT is not configured with software to hide the device or data traffic through the device from authoritarian regimes. The MESS-KIT has no tools to protect individuals whose online activities could lead to arrest in a host nation where free speech principles do not conform to US or EU standards, and it should not be used in this way without substantial modification.

IA STRATEGY
CMOs—and in particular counterinsurgency operations—require the military and civilian partners to accept greater risk than regular warfare. The MESS-KIT introduces open information flows between partners, and therefore introduces new or enlarged risks than traditional operations. The IA strategy for the MESS-KIT is to **reduce** risks associated with information sharing, but not to **eliminate** them.
The system will approach information security in three ways:
1. Wireless Field Operations (WFO) Wireless Field Operations mode enables technologically adept organizations to build MESS-KIT nodes to give to partner organization with less technological infrastructure, and to establish WiFi shots to the partner from another location (in the absence of conventional internet connections). An example of how this would work would be to send RSS (Really Simple Syndication) feeds through WEP-encrypted WiFi shots, enabling members of the MESS-KIT network to exchange information via RSS/XML-based feeds.
2. Wired Office Operations (WOO) In cases where WiFi is impractical or would be easily compromised, wired access to partners is possible. The WOO method ensures that physical access to the network is required to access data feeds.
3. Physical Data Transfer (PDT) In cases where security concerns outweigh the benefits of RSS feeds to exchange data between partners, virtual machines can be suspended and saved to memory devices. Personnel from any organization can carry the virtual machine to another site, where it can exchange RSS feeds in a closed network environment with the MESS-KIT instances at the second site. Similarly, specific data sets can be saved to external memory devices and transferred between machines.

THREATS
Misinformation
Because MESS-KITs will be placed into the operational control of CMO partners, and because not all partners are favorably disposed towards the military, it is possible that partners could inject misinformation into the MESS-KIT system. The system is not designed for automated detection of misinformation; it relies on humans to distinguish truth from falsity.
Information Leakage
Information about non-combat projects and programs conducted by CMO partners will be contained on MESS-KITs. Some information will be exchanged between MESS-KITs, creating redundant copies of certain files. This information could leak into areas beyond the CMO partnership. The cost-benefit ratio between the increased coordination of unity of effort and the increased risk to projects/programs through information leakage is

something to be constantly considered. Thus, in a way, information assurance is a misnomer. There are no ironclad information safety guarantees.

SECURITY
Partner Selection Rules
Partners should be chosen within a network of trusted existing relationships. Partners who decide to grant a new partner a MESS-KIT should be comfortable adding the partner as a node on the network. Trust is the key metric here, which is left to the judgment of the person distributing the MESS-KIT.
Authentication and User Account Management
Each MESS-KIT will be configured with 100 possible user accounts with a username/ password. When the MESS-KIT is deployed, a facilitator will assign one of the preconfigured accounts to an individual member of the receiving organization. This set of credential controls access to the suite of software contained inside the MESS-KITs virtual machine and also links a user account to the data entered on the machine and the log entries of actions on the machine. These credentials can be revoked through physical access to the virtual machine. At this time, remote access to the virtual machine is not planned, nor any functionality that would enable remote revocation of credentials.
Data Flows
Data will flow over wireless (WiFi) connections using commercial-grade encryption. In addition, all data will be transferred using 128-bit SSL (Secure Sockets Layer) encryption over HTTPS (Hypertext Transfer Protocol Secure). That said, because all encryption algorithms for wireless network can be cracked, it is possible for advanced insurgent elements and other unfriendly organizations to be able to track data flows between two or more MESS-KITs. This is another unavoidable risk inherent to conflict situations.

CONTINGENCIES AND CONTINUITY PLAN
Backup and Recovery
The MESS-KIT should be backed up regularly. The frequency for this backup will be determined by the individual partner who has physical access to the MESS-KIT. Backups will use the virtual machine's backup system, which enables a user on the device to backup the current state of the virtual machine to a second memory device, such as a CD, DVD, external hard drive, or USB stick. Backups can be performed manually or can be placed on a regular automated schedule. These backups are also portable: virtual machines can be opened on another machine, including personal laptops. In this way, should a device ever have a hardware failure, the last backup of the virtual machine can enable continuous operation.
System Theft/Compromise
Systems may be stolen or lost. There is no plan to remotely lock a stolen system or wipe its hard drive clean. Users should protect the systems as best as possible. Losses will be dealt with on a case-by-case basis. Because user accounts are preconfigured, it will be possible to track compromised accounts.

Support and Training

From Wiki

Jump to: navigation, search
SYSTEM SUPPORT
Because the MESS-KIT system is composed of commercial-off-the-shelf hardware and commercial-off-the-shelf AND free-and-open-source software, all hardware and software components are field maintainable. Those who wish to employ the units will be required to train teams in the basic field repair of the MESS-KIT, to include:

• Replacement of internal memory storage device, including backup and restoration of data.
• Replacement of external memory storage device, including backup and restoration of data.
• Updates to Ubuntu operating system.
• Updates/replacement of MESS-KIT virtual machine.
• User account administration.
• Security Training, including how to setup users and groups and protect the box against physical theft.

TRAINING

Users of the MESS-KIT will receive training via video and/or PDF documents that explain the basic operation of the system.

Software Guide

From Wiki

Jump to: navigation, search

I. Introduction

This page offers descriptions of MESS-KIT software and offers instructions for use of the MESS-KIT software suite.

Before you begin an investigation of the software, please refer here for a quick introduction to the Virtual Machine hosting software; a necessary component of the MESS-KIT system.

The MESS-KIT also uses an open-source "platforming" system called JumpBox. JumpBox is a company that makes ready-to-use packages of open source software. They allow open-source software, which is often time consuming and difficult to install, to be used more seamlessly. JumpBox simplifies server software deployment with "pre-built" and "pre-configured" software applications packaged that automatically take care of the grunt work of open-source installation, thus allowing for the use of otherwise complex applications by users with minimal technical knowledge. Think of JumpBox as an entirely constructed automobile. It's ready to drive. Technical or mechanical work was taken care of elsewhere. And a knowledge of which is not necessary for the successful "start-to-finish" use of the car; or, in our case, the software.

Refer to the JumpBox Instructions page for important JumpBox documentation including data backup instruction.

II. MESS-kit Software Suite Information "Quick Reference":

III. Detailed instructions for basic MESS-KIT software functions:

Drupal.
KnowledgeTree.
DimDim.
MediaWiki.
Wordpress.
Moodle.
GeoCommons.

FAQ Page

From Wiki

Jump to: navigation, search

1.) Can my organization use any of the MESS-KIT features without an internet connection?

Most of the features of the MESS-KIT do not require an internet connection. The system, however, does require local networking. This can be as simple as a broadcasting a WiFi signal from the MESS-KIT server, or could be something as complicated as a WiMax system or point-to-point WiFi. An internet connection will allow remote access and remote backup.

2.) I am not a "tech-savvy" user. Will this inhibit my succesful use of any of the software installed on the MESS-KIT?

There are two types of users for the MESS-KIT, the administrator and the end-user. The administrator sets the kit up, and maintains it. Efforts have been made to make this as simple as possible, and is much easier than traditional systems administration. No command line skills are necessary. Someone with an enthusiasm for technology and basic computer literacy should be capable of administering the MESS-KIT.

The end-user needs to know how to operate a web browser. The systems on the MESS-KIT follow standard web design, and look and feel like normal web sites.

3.) I am confused. Should I set up a blog with Wordpress or Drupal?

The MESS-KIT was designed to be flexible around your organizational needs. If you just want a blog, Wordpress is a good option. If you want to set up a social networking site for a whole team, Drupal is what you want.

4.) I am very familiar with the Microsoft Office software suite. Can I use that on my MESS-KIT?

If you would like to manage large amounts of documents I'd recommend the KnowledgeTree system.

5.) How susceptible is my MESS-KIT to viruses? Is the software resilient?

The end-users of the MESS-KIT interact with it through a browser, which reduces the possibility of viruses. End-users should be aware of normal security precautions, such as having good passwords and running antivirus software on their systems.

6.) What troubleshooting protocols should my organization enter into if we begin to experience software malfunctions?

Most of the systems on the MESS-KIT have commercially available support. For instance KnowledgeTree is free and open software, which has a for-profit company behind it. http://www.knowledgetree.com/

7.) What security features are in place to protect my data?

The MESS-KIT uses only secure internet communication protocols, you'll notice in the browser bar only the 'HTTPS' setting is used. This encrypts all traffic across the MESS-KIT network. All of the systems on the MESS-KIT have standard internet security, and use passwords to protect their users.

8.) When I upload documents to KnowledgeTree, where do they go?

To a database within the MESS-KIT.

Technical Documentation

From Wiki

Jump to: navigation, search

I. Mess network setup and configuration

The idea here is that MESS-KIT will be used in various places with limited or no upstream network connectivity. To that end we use what we will call a mess server to create a mess network. The idea of the mess network is any address ending in .mess is local to the network and will not require any external internet access to use. However, if there is internet access that will be available as well. Here is the documentation relevant to making this happen.
a. Ubuntu 9.10 on Lenovo X100e: We are using a Lenovo X100e for our development server. Here is the why and how.
b. .mess TLD: Setting up a .mess top level domain name on Ubuntu
c. MESS Network: This is how to setup a MESS Network on Ubuntu
d. Virtual Machine: This is how to install and run a virtual machine environment on Linux
Retrieved from "http://192.168.1.50/index.php/Technical_Documentation"

History of the MESS-KIT

From Wiki

Jump to: navigation, search
History of the MESS-KIT
The first MESS-KIT was a Mac Mini which was taken to Afghanistan during the August 2009 Presidential Elections. The machine was a 'sandbox' for several experimental web-based services that were being tested out. The original goal was to have a small web server which could be taken to the field to provide local web services.
Why a field server? Field users often cannot install new software on their machines without the permission of some guy at a desk on another continent. Web sites are very popular, because they do not require any installation and are easy to use. However, internet connections are rare. A field server makes it possible to serve up websites over local networks.
The first MESS-KIT had a custom mash-up of the following services:

- Google Fusion server[1] -- Serving up satellite imagery
- GeoCommons[2] --Organizing and mapping GIS data
- OpenStreetMaps[3] -- Creating and displaying street maps
- WalkingPapers[4] -- Creating paper streets maps which are easily digitizable
- Sahana [5] -- Disaster management and logistics
- GeoChat[6] -- SMS and geospatial messaging

The idea is these services, run locally on inexpensive hardware, can be used to more rapidly stand up information sharing capabilities when larger networks are down.
The experiment was successful, in that the prototype was used by the team in Afghanistan. However, having a large number of services on a single server requires systems administration skills, and the design was reworked after the event to make it easier to allow operational experimentation.
Some documentation from the first prototype:

"The starting point was 50 cm imagery of Aghanistan, released by the National Geospatial-Intelligence Agency. Todd Huffman, known to me from the Beer for Data program, negotiated free use of the invaluable imagery. OpenStreetMap's response to Gaza demonstrates just one application of the power of easily available imagery. The US government, and many other governments, purchase this imagery with our tax money, and it's totally reasonable and to be expected that such imagery should be put to its widest possible use in times of crisis."

The diagram of the system at Camp Roberts
--There is a Kitfox. More on OpenStreetMap at Camp Roberts[7]

Gearing up for the elections themselves we've already started ingesting data from Todd and folks on the ground in Afghanistan. Data will be geo-referenced and mapped with the Mac-Mini GeoIQ appliance for local use then federated up to public GeoCommons for wide spread dissimenation. We'll be publishing the most pertinent maps to a dashboard throughout the elections. So far we've been georeferencing data from UNHCR district profiles, JICA security summaries, polling locations, tribal boundaries, etc.

Screen Shot from the Geocommons appliance
--Camp Roberts Exercise and the Afghanistan Elections: Creating a Geo-Stack for Humanitarian Relief[8]

First challenge was the actual deployment of GeoChat. Since we were looking forward to develop several mashups on the fly, we took with us a separate version of the server so we could tweak it as much as needed for the sake of the exercise without modifying the already running production server (which, by the way, you are all welcome to use). We would also be deploying a local gateway, which is nothing more than a simple client installed in a laptop connected to a cell phone that relays messages from and to the server, as the US shared gateway was in use at the production server. The huge problem was we did not get any signal on the base.
--Camp Roberts RELIEF Recap[9]

Out in the field at Camp Roberts

The Google Earth Enterprise team knew we could help out, and we processed the imagery for Todd through Google Earth Fusion, and then published the data as a map, and 3D globe to a Google Earth Enterprise Server running in an Ubuntu Virtual Machine connected to a mac-mini which was provided to Todd to run GeoCommons by FortiusOne.
--Preparing for Afghanistan Elections and Humanitarian Efforts[[10]]

Out in the field at Camp Roberts

"Data-sharing.
A key objective of STAR–TIDES is to promote the sharing of not only processed information, but also of underly- ing data so that others can create value in ways that may not have occurred to the original data own- ers.30 After the August 2009 Camp Roberts experiments and experi- ences in Afghanistan, one of the participants outlined three principles for data-sharing.

- Create immediate value for anyone contributing data; when users contribute data, they should get an immediate return on that investment.
- Make contributor data available with improve- ments; any data that goes in should be available to download back out again. Furthermore, data should come back better than when entered.
- Share derivative works back with the data-sharing commu- nity; urge users who create derivative works from shared data to contribute their products back to the group."

-- Linton Wells II, Walker Hardy, Vinay Gupta, and Daniel Noon STAR–TIDES and Starfish Networks: Supporting Stressed Populations with Distributed Talent. Defense Horizons. Center for Technology and National Security Policy December, 2009. National Defense University[11]

A screen shot from the United Nations Foundation Report
A week-long exercise to test UAVs for crisis response— the first of its kind—took place in California in August 2009. The exercise combined the use of UAVs with SMS, VHR image processing, and open source GIS applications and was held at Camp Roberts in California. The exercise focused on two scenarios—stability operations in Afghani- stan and planning for a natural disaster in Central America.
Participants included geographers, software developers, and crisis mapping experts. They developed a novel approach to information collection by using UAVs, SMS, low-bandwidth satellite connec- tions, and high-resolution satellite imagery of Afghanistan. For example, they integrated Open Street Map's new Walking Papers application and combined this with the images taken by UAVs. Walking Papers works by enabling a user to down- load any part of a map to a printable file, which includes a bar code. Users can then annotate the hard copy map with a pen or pencil when they are out in the field. They can then scan the annotated map and upload the new data online. This provides a method of mapping field data even when Global Positioning System (GPS) units are not available and network connections are down. It also enables local people to point out spots on the paper map.

Guide to using the MESS-KIT in the field

From Wiki

Jump to: navigation, search
There are several traits of the MESS-KIT which lend it to field usage.

- Systems can be migrated between hardware
- Systems can be scaled with locally available hardware
- Systems can be preconfigured before heading to the field
- Systems can be backed-up easily

Retrieved from "http://192.168.1.50/index.php/Guide_to_using_the_MESS-KIT_in_the_field"

Migrated between hardware

From Wiki

Jump to: navigation, search
One of the benefits of the virtual machine architecture of the MESS-KIT is the systems can be 'suspended' while running. A VM does not need to be shut down before being suspended, and when it's 'resumed' it will be at the exact same point where it left off. This feature is extremely useful in the field, because there often isn't the luxury of shutting things down and doing proper migration.
Here's a video of suspending a VM in the middle of a long tiling session: <object width="480" height="385"><param name="movie" value="http://www.youtube.com/v/Oj8CrEQXiwY&hl=en_US&fs=1&"></param><param name="allowFullScreen" value="true"></param><param name="allowscriptaccess" value="always"></param><embed src="http://www.youtube.com/v/Oj8CrEQXiwY&hl=en_US&fs=1&" type="application/x-shockwave-flash" allowscriptaccess="always" allowfullscreen="true" width="480" height="385"></embed></object>

The VM folder can be copied to another machine with VMWare, and restarted. To minimize interruptions, manually set the IP addresses. For more information about networking, see Set Static IP Address
From the VMWare Support Files
"Suspending and Resuming Virtual Machines
The suspend and resume feature is most useful when you want to save the current state of your virtual machine, then pick up work later with the virtual machine in the same state it was when you stopped.
Once you resume and do additional work in the virtual machine, you cannot return to the state the virtual machine was in at the time you suspended unless you took a snapshot when you suspended.
To preserve the state of the virtual machine so you can return to the same state repeatedly, take a snapshot. For details, see Taking Snapshots.
The speed of the suspend and resume operations depends on how much data has changed while the virtual machine has been running. In general, the first suspend operation takes a bit longer than subsequent suspend operations do.

When you suspend a virtual machine, a file with a .vmss extension is created. This file contains the entire state of the virtual machine. When you resume the virtual machine, its state is restored from the .vmss file. The .vmss file cannot be used to resume a virtual machine again from the original suspended state.
Note: You should not change a configuration file after you suspend a virtual machine, since the virtual machine does not resume properly if the configuration file is inconsistent with the suspended virtual machine. Also, you should not move any physical (raw) disks that the virtual machine uses. If you do, the virtual machine cannot access its virtual disks when it resumes.
To suspend a virtual machine:
1. If your virtual machine is running in full screen mode, return to window mode by pressing the Ctrl-Alt key combination.
2. Click Suspend on the VMware Virtual Machine Console toolbar.
3. When GSX Server has completed suspending the virtual machine, it is safe to close the console.
File > Exit
To resume a virtual machine that you have suspended:
1. Launch the VMware Virtual Machine Console and choose a virtual machine you have suspended.
2. Click Resume on the console toolbar.
Note that any applications you were running at the time you suspended the virtual machine are running and the content is the same as it was when you suspended the virtual machine.
You can suspend and resume a virtual machine with the management interface. See Changing a Virtual Machine's Power State from the Management Interface.
You can also set the configuration of each virtual machine so the file that stores information on the suspended state is saved in a location of your choice." [1]
Retrieved from "http://192.168.1.50/index.php/Migrated_between_hardware"

Scaled with locally available hardware

From Wiki

Jump to: navigation, search
Under normal conditions locally sourced hardware can be difficult to integrate into an IT workflow. For a system might be running Windows, and what's needed is Linux, and regulations prevent re-installing the operating system. There might not be an internet connection for downloading the specific Linux drivers needed. Using the VM architecture avoids many of these issues, and makes it easier to integrate hardware found in the field, because the hardware need only be able to run the virtual machine environment.
Example Use Case: A user goes into the field with a MESS-KIT consisting of a laptop and router. They set up three services on the laptop, which are available to other machines on the network via browsers. As the user load increases there's demand for another service, and for faster service. A computer is acquired locally, and VMWare installed on it. The service is suspended on the original machine, the files transferred over, and restarted. To users on the network, there was little interruption in service, and more computational capabilities have been made available.

The MESS-KIT configuration with three web services running on the netbook computer

The MESS-KIT configuration with four web services running, two on the original hardware and two on a locally sourced system.

Preconfigured before heading to the field

From Wiki

Jump to: navigation, search
Taking IT to the field faces three problems

- You don't know what you're going to need until you get there
- Once you're there you don't have time to build it
- There's probably not internet

The concept behind the MESS-KIT is one can pre-configure systems and carry a library into the field. At any give time only three or four might be necessary, but it's nice to have a good side-deck.
For instance Todd Huffman is heading into Afghanistan, and has a large library of PDF's about the country. He's dumped them into a KnowledgeTree instance, where they've been indexed, and built into a search engine. If people have an interest in the documents the VM can be fired up, where they can search through and exported to their own computers over the browser.

Preconfigured systems can be prepared in this fashion, such as geospatial services, video chat, social sites, and more. Over time an organization will build a library of useful services, which can be exchanged with others in the field.
Retrieved from "http://192.168.1.50/index.php/Preconfigured_before_heading_to_the_field"

Backed-up easily

From Wiki

Jump to: navigation, search
There are several ways one can back up a virtual machine.
The most obvious is through conventional back up systems. There are a variety of software packages which can be installed on the virtual machine itself to back up the systems.
Snapshots are another convenient way to back up the virtual machines. The benefit of a snapshot is that the system can be restarted from the point of backup within minutes. Taking snapshots is simple, and can be automated in the VM environment. For more details, see taking snapshots
On some virtual machine configurations, such as those by JumpBox, just the unique data can be backed up which saves on storage space. The data is stored in a large text file in an XML format, and is partially human-readable, which can be useful. To restart the machine from backup requires having a JumpBox of the same type. For more details, see backing up JumpBoxes

Best Practices

From Wiki

Jump to: navigation, search
Transporting VMs -- Moving VMs between machines can be made much easier. Before 'setting to seed', follow these steps:

- Shut-down the VM -- You can transfer a running VM, but it's better not to unless you need to

Then, in the settings, scale back the requirements for the VM, in case the system is restarted on a lower-end machine

- Use 32-bit VMs Unless you're sure there's a 64-bit machine on the other end
- Use 1 core Unless you're sure there's a multi-core machine on the other end

Speed -- If your VM is getting a lot of traffic or doing computationally intensive jobs like tiling imagery, there are some settings you can adjust which really increase the speed.

- Preallocate disk space
- Increase the memory
- Add more processors

Field-specific Issues -- Here are some tips to standing up the MESS-KIT in austere conditions. Yes, they seem obvious, but it's amazing how obvious gets missed.

- Have enough power strips and uninterruptible power supplies
- Bring your own router

Users

From Wiki

Jump to: navigation, search
There are three levels of people interacting with the MESS-KIT
Chef -- The person who designs and makes the first iteration of a given MESS-KIT.

- Skill level -- Systems administrator level skills

Server -- The field administrator of the MESS-KIT.

- Skill level -- Basic knowledge of Unix command line and network troubleshooting skills

Diner -- The end user of the MESS-KIT

- Skill level -- Basic knowledge of internet browser function, and training on the specific Utensil they'll be using.

Virtual machine environment

From Wiki

Jump to: navigation, search
Refer below for information regarding the two types of virtual machines:

A virtual machine (VM) is a software instance of a machine that executes tasks like an actual, *physical*, machine.
The term "virtual machine" was originally defined by Gerald J. Popek and Robert P. Goldberg as "an efficient, isolated duplicate of a real machine".
Virtual machines are separated into two major categories based on their use and degree of correspondence to any real machine.

a. A *process* virtual machine is designed to run a single program, which means that it supports a single process. An essential characteristic of a virtual machine is that the software running inside is limited to the resources and abstractions provided by the virtual machine—it cannot break out of its virtual world.
Example: A program written in Java receives services from the Java Runtime Environment (JRE) software by issuing commands to, and receiving the expected results from, the Java software. By providing these services to the program, the Java software is acting as a "virtual machine", taking the place of the operating system or hardware for which the program would ordinarily be tailored.

b. *System* virtual machines (sometimes called hardware virtual machines) allow the sharing of the underlying physical machine resources between different virtual machines, each running its own operating system. The software layer providing the virtualization is called a virtual machine monitor or hypervisor. A hypervisor can run on bare hardware (Type 1 or native VM) or on top of an operating system (Type 2 or hosted VM). A system virtual machine provides a complete system platform which supports the execution of a complete operating system (OS).

The MESS-KIT system will utilize this latter type. Here is a screenshot of what the MESS-KIT "process" VM should look like upon start-up:

Screenshot

Running web service is more complicated than running normal programs. Usually you need a system administrator to set web-service up and to administer it. That can become expensive or impossible in some situations. MESS-KIT aims to solve these problems and work towards the goal of increasing the efficiency and effectiveness of cross-organization communication in an effective way even without the internet. Part of the inspiration for the MESS-KIT project was found in watching people go to the field and talk to each other in the same building using the internet. For emphasis, their message goes out of their computer, through the local network, TO SPACE, back down to earth in the United States, talks to the internet, where it then goes back TO SPACE, then back down to earth, to the local network and to the other person. Why should we have to send a message to space just to talk to someone in the same building? That's expensive and slow and showcases a single point of failure for communications. The MESS-KIT is meant to be a piece of infrastructure to support basic web interactions without an internet connection. This function is strongly facilitated by the JumpBox platform and open-source soft-ware central to the system.

The main advantages of system VMs are that:

-multiple OS environments can co-exist on the same computer, in strong isolation from each other.
-the virtual machine can provide an instruction set architecture (ISA) that is somewhat different from that of the real machine.
-application provisioning, maintenance, high availability and disaster recovery are easily executed tasks.
The main disadvantage of a system VMs is that:
a virtual machine is less efficient than a real machine when it accesses the hardware indirectly. And this efficiency problem can effect some performance functions.

The MESS-KIT will rely heavily on virtual machine (VM) environments. Most all of the programs to be used as part of the MESS-KIT system (with the exception of SAHANA and GeoCommons, for instance, as they are web-based programs) will use a process VM called "VMWare Player." Refer below for instructions on a few important features of "VM Player":

1. Starting a program through VM Player is straightforward. Choose the program you'd like to use from the list that populates the left of the VM Player's screen:
Screenshot 2

2. After you have chosen the program you would like to use (in this example case we are using KnowledgeTree), you will come to a screen that looks like this. Choose the "Application" IP address and type it in to your address bar:

Screenshot 3

3. After you have typed in the necessary IP address you will come to your software's home-page. At that point, all you will need to do is enter your user information and begin use:

Screenshot 4

There are a number of virtual machine environments available. Discover what is out there by following these links:
VMWare is a commercial product with numerous products ranging from the desktop to server farms. They offer several free products.
VirtualBox is an open source system that runs on Windows, Linux, and OS X.
Microsoft Virtual PC is a virtualization program for microsoft Windows operating systems.

Hardware

From Wiki

Jump to: navigation, search
Details on specific hardware devices:
Power Supply Replacement
Network Attached Storage
Communication Methods
Minimum Mac system requirement for VMware 3:

- Any Intel® Mac.
- Minimum 1GB of RAM (2GB RAM recommended)

- 700MB free disk space for VMware Fusion and at least 5GB for each virtual machine
- Mac OS X 10.5.8 or later; Mac OS X 10.6 or later
- Operating system installation media (disk or disk image) for virtual machines

Refer to this technical resource center link for a more in-depth hardware compatibility guide:
http://www.vmware.com/resources/compatibility/search.php.