ActioNews

ActioNet solutions are built on **People, Innovative Processes, Technology** and **Partnership**. ActioNet has established an outstanding track record of creating continuously forward-looking, cost-effective IT solutions, meeting such Federal mandates as 'Cloud-First' initiatives. Our ActioNetCloud® family of service offerings include:

- **ActioNetDesk™**
- **ActioNetAgile™**
- **ActioNetHosting™**
- **ActioNetMobility™**
- **ActioNetCyber™**
- **ActioNet360™**

For a complete list of ActioNetCloud™ Solutions, visit www.actionet.com/Solutions/ActioNetCloud.asp

ActioNet's Core Values center on Customer Service, Employee Growth and the Quality of our Work. We continually invest in our people and our capabilities with a continual process improvement focus based on ISO 20000, ISO 27000, ISO 9000, HDI and CMMI® Level 3. We are proud to have many certified staff:

- 500 ITIL Certified
- 100 PMP Certified
- 80 DoD 8570 Compliant
- 35 ScrumMasters
- 24 AWS Certified Technical

The key to successful transformation into a performance-based, customer-focused organization is clearly defining the current state of the organization and building a detailed roadmap for improving service delivery.

Ashley W. Chen
President & CEO
703.204.0090
info@actionet.com

ActioNet, Inc.
2600 Park Tower Drive
Suite 1000
Vienna, VA 22180
www.actionet.com

ActioNet

Establishing Governance for Mission-Critical Data

continued from page 3

ActioNet was charged with an Enterprise Shared Services (ESS) project to work with the Agency to merge all the disparate sources of data into a centralized SharePoint repository. Its charter includes both the creation and the governance of an Enterprise SharePoint Environment. It will provide content and document management features of versioning, collaboration, security and workflows to the enterprise, as well as development of new projects and applications to support Agency Operations.

The first task of the project was to set up a Program Governance Structure. This is a crucial component of project initiation, as it involves communicating with and getting executive buy-in for the project. Accordingly, we held meetings with a working group comprising stakeholders from each Agency organization, and explained the goals of the project, expected benefits and timelines.

In consultation with the working group, we set up an ESS Executive Board, Change Control Board and a Program Management Office (PMO). Each ESS entity's Terms of Reference was developed, and roles and responsibilities were formalized.

Three categories of new project requests were identified and their approval workflows were created.

CATEGORY	CHARACTERISTIC	APPROVAL
Category 1	Enterprise-wide scope, Cross-Program Impact	ESS Executive Board
Category 2	Program Specific Scope, Limited Custom Development	ESS Change Control Board
Category 3	Out of the Box Collaboration Sites and Workflow	ESS PMO

Templates are being developed for new project requests, new user requests, and each stage of the project lifecycle. ActioNet is leveraging several best practices and frameworks such as Project Management, COBIT, ITIL and SDLC. Coding standards and Standard Operating Procedures are being developed.

The PMO drafted the Information Architecture of ESS SharePoint site and the various Office subsites. Initial development of the home page, global navigation and subsites has been completed. A Google drive to SharePoint migration prototype for a Program Office is being worked on as a proof of concept. The document life cycle comprises multiple versions of documents, each going through its own review cycle, and then being consolidated into final approved documents.

As per the mandate from Agency management, all existing data sources must migrate to ESS by the next Fiscal Year. The ESS PMO is working each Organization to come up with a migration schedule within the mandated timeline.

The benefits to the Agency include: secure and timely access to information, one central repository, streamlining of IT assets, and optimization of service delivery costs. The ActioNet team is excited to be leading this venture, by planning, executing and supporting an enterprise-wide SharePoint service offering from the ground up.

The forecast for the ESS project is set fair, and sunny days are projected ahead.

• • • • • • • • •

ActioNet Sponsors Veterans of America Clothing Drive 2/21-3/17

ActioNet

Veterans of America Clothing Drive

"Never again will one generation of veterans abandon another."

February, 21-March 17, 2017
ActioNet HQ Reception Area
POC: Michelle Barnes
703-204-0090x102
mbarnes@actionet.com

ACCEPTABLE ITEMS
All men's, women's, children's and infant's clothing including:

Raincoats and Overcoats
Dresses
Shoes and Boots
Ties
Shirts, Blouses, Sweaters
Pants and Jeans

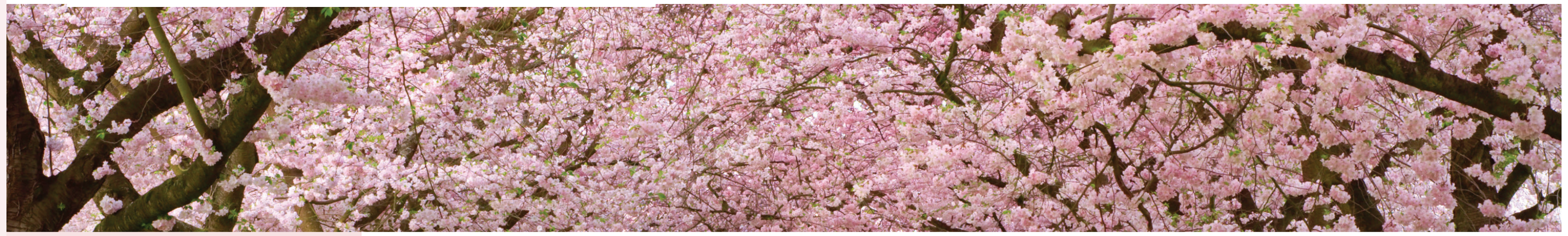
T-shirts
Formal Wear
Hats and Gloves
Handbags and Purses
Belts
Socks

ActioNet collected clean, gently used Clothing as part of the Veterans of America Clothing Drive. Clothing of all shapes and sizes are welcome. Veterans of America Clothing Drive is dedicated to distributing reusable coats, free of charge, directly to local Veterans of America. This was a great opportunity to help those in need right here in our communities during the Spring season.

"Helping Veteran's, Communities, and those serving in harms way". Veterans of America's mission is to promote and support the full range of issues important to all veterans. Veterans of America will be there for as long as it takes to make sure that those who serve our country receive the care and respect they have earned. Veterans of America is a respected charity that gives aid to all of America's veterans, not just those of a particular age group or war.

ActioNews

SPRING 2017
THE NEWSLETTER OF ACTIONET



Turning **VISION** into **ACTION®**

PRESIDENT'S NOTE

Dear Friends,

In this issue of ActioNews, we discuss the deployment of a secure multi-layer access solution for Application Hosting Environments, as well as leveraging Enterprise Shared Services to improve the management of IT Assets and Data.

As part of our Community Activities, ActioNet is supporting the Veterans of America Clothing Drive by donating clothing of all shapes and sizes between 2/21 – 3/17.

Ashley W. Chen
President & CEO

IN THIS ISSUE

Securing Privilege Access Using ESAE

By Randall Flynn, Sr. Enterprise Architect

As a part of a major Information Technology Support Contract servicing the Office of the Chief Information Officer (OCIO), ActioNet maintains and administers the Application Hosting Environment (AHE). AHE is essentially an Infrastructure as a Service (IaaS) offering with bundled support services through the OS layer. This model allows offices throughout the Agency to request, and have provisioned systems for specific organization use that meet all security and maintenance requirements for attaching to the network. Customers have no need to have subject matter expertise beyond their specific application as the OCIO through ActioNet maintains all aspects outside the application to include network transport, shared services, security down to the OS, and identity management.

In 2013 ActioNet successfully demonstrated to the OCIO that an attacker, once in to the Production Forest could raise their privileges from a standard user or service account up to Enterprise Administrator. Based on this finding our customer requested that we begin design of a way to mitigate this type of attack. ActioNet worked very closely with our partners at Microsoft and together we developed plan. We created a design to address with the OCIO's specific needs using a custom-tailored implementation of the Enhanced Security Administrative Environment (ESAE). ESAE provides an isolated, secure administration environment for Active Directory credentials. The environment is intended to manage and protect Tier 0 Enterprise Administrator (EA) and Domain Administrator (DA) accounts on Internal Forests and Domains. Microsoft defines Tier 0 in the Active Directory Administrative Tier model as "Direct Control of enterprise identities in the environment. Tier 0 includes accounts, groups, and other assets that have direct or indirect administrative control of the Active Directory Forest, Domains, or Domain Controllers, and all the assets in it. The security sensitivity of all Tier 0 assets is equivalent as they are all effectively in control of each other." The ESAE uses an architecture built on fundamental security principles and industry leading technologies. The ESAE is designed to thwart cyber attackers' business impact on domain-joined Windows machines by mitigating credential theft techniques as well as several other known attack techniques. The solution focuses on credential theft mitigation, credential hygiene, and enhanced operational security policy.

> "... an attacker, once in to the Production Forest could raise their privileges from a standard user ... to Enterprise Administrator."

continued on page 3

ActioNews, the newsletter of ActioNet, Inc. is published to provide examples and applications of cutting edge IT topics and practices.

ActioNews is published quarterly (March, June, September and December) as a service to its staff, customers, and potential customers.

ActioNews Staff

Lead Designer

Lynda D. Pitman

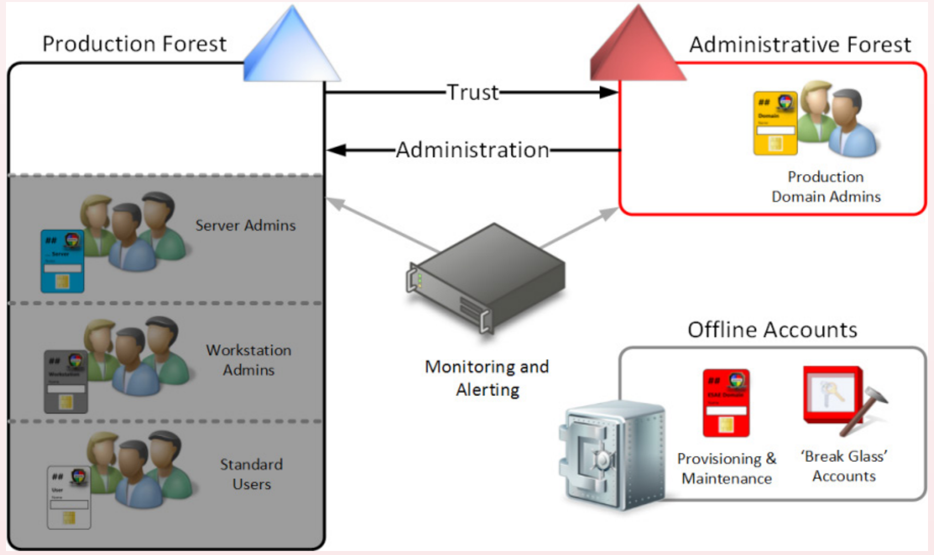
Contributing Authors

Randall Flynn
Mohan Pillalamarri

> "…the ActioNet Team, as part of our continual improvement process, began looking to ways to further increase security for our customer."

Securing Privilege Access Using ESAE

continued from page 1



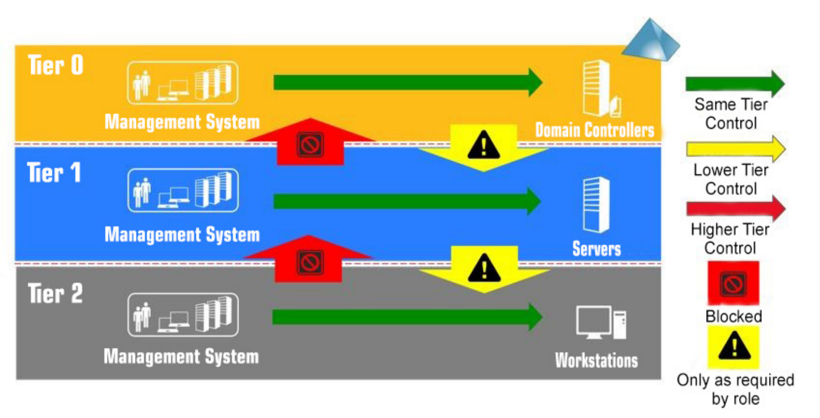
To provide clarity in how the system works from this point forward the ESAE forest will be labeled 'Administrative Forest' and the internal forest will be labeled 'Production Forest'. ESAE functions by creating a separate Active Directory (AD) Forest (Administrative Forest) which is logically locked down using security technologies such as IP Security (IPSEC), AppLocker, and Two Factor Authentication using a private Certification Authority (CA). A Selective Trust is created between the Administrative Forest and the Production Forest. The Administrative Forest CA also provides certificates to each object within the Administrative Forest to allow the use of IPSEC across the environment. EAs and DAs use clean source entry points called Privileged Access Workstations (PAWs), which are members of the Administrative Forest to administer the Production Forest. To authenticate the PAWs, admins use Multi-Factor Authentication (MFA) through smartcards issued through the Administrative Forest CA. This ensures no trust of outside systems.

The Administrative Forest contains separate user accounts for Production Forest Administrators (Gold Card Admins) and require the use of Smartcards and PAWs to access resources. Gold Card Admins have no rights within the Administrative Forest. Gold Card Admin accounts from the Production Forest are deleted, the Gold Card Admin accounts from Administrative Forest are added to Production Forest groups. Administrative Forest Administrators (Red Card Admins) have no administrative rights into the Production Forest. This methodology creates separation of duties, reduces the likelihood that domain credentials are compromised through user rights escalation, and provides a layer of two person control for changes to the environment in which domain administrators operate.

The PAWs, and the servers inside of the Administrative Forest have no external connections to any other systems aside from the one way selective trust with the production domains, and a simple 443 outbound only rule on the patch server allowing the downloading of MS patches.

During implementation of the Administrative Forest, ActioNet worked to clean up the Production Forest, removing unnessary accounts and reducing priviledges as seemed necessary. Once the implementation of the Administrative Forest infrastructure was completed, tested and authorized, ActioNet worked with all customers that held DA access or higher throughout all domains in the Production Forest. Users accounts were created in the Administrative Forest, along with the issuance of SmartCards and PAWs. At that time the Production Forest accounts were disabled while each user performed functionality testing of the new Administrative Forest account. Once all issues were resolved Production Forest administrative accounts were removed.

Following the successful implementation of this project, the ActioNet Team as a part of our continual improvement process, began looking to ways to further increase security for our customer. We again reviewed Microsoft's Active Directory administrative tier model, this time focusing on what Microsoft considers Tier 1 assets. Microsoft defines Tier 1 as having "control of enterprise servers and applications. Tier 1 assets include server operating systems, cloud services, and enterprise applications. Tier 1 administrator accounts have administrative control of a significant amount of business value that is hosted on these assets. A common example role is server administrators who maintain these operating systems with the ability to impact all enterprise services." Tier 1 assets include many high value enterprise capabilities, thus they are high value targets for attackers. Some of the most critical applications we identified within our Tier 1 include Virtualization (vCenter, Hyper-V, Citrix), Configuration Management (BigFix, SCCM), Policy (McAfee ePO, Symantec DLP), Antivirus, Storage, and Monitoring among many others.



Based on the recommendation by Microsoft to not include any additional functions beyond the initial design we recommended creating a Management Forest where a separate Infrastructure Forest can be created to provide secure, multi-factor credentials for infrastructure items, and to simplify the environment. Separate Application Forests within the Management Forest are recommended for application users. Compared to the current environment, where UN/PW credentials are stored in numerous, un-secured locations including the Production Forest. The Management Forest will provide a central, more manageable, and easily secured solution for multi-factor enabled accounts. Admin laptops will provide trusted and locked down end points for infrastructure admins, and jump boxes for application owners. Accountability will be easier, as Cyber Operations, ISSOs, and Information Assurance Vulnerability Management (IAVM) teams will be able to focus on a single entity, compared to the numerous of authentication sources which exist. The implementation of the Management Forest infrastructure will be completed in the next fiscal year.

Additional information about the concepts used to establish these environments are available from Microsoft.

Securing Privileged Access Reference Material

https://technet.microsoft.com/en-us/windows-server-docs/security/securing-privileged-access/securing-privileged-access-reference-material

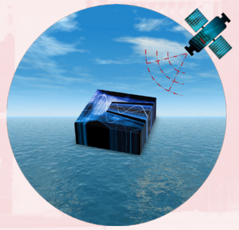
Privileged Access Workstations

https://technet.microsoft.com/en-us/windows-server-docs/security/securing-

• • • • • • • • •

Establishing Governance for Mission-Critical Data

By Mohan Pillalamarri, Project Manager



The next time you look at the weather forecast, think about all the entities that work together seamlessly in the background to bring you the temperature in your neighborhood. There are advanced weather satellites in space that are tracking the weather systems, ground offices that work with NASA to help launch satellites in space, and Data Centers that help process the satellite images that are continually being beamed back to earth.

The National Oceanic and Atmospheric Administration (NOAA) is the federal agency that monitors the earth's climate, environment and weather. Secure and timely access to global environmental and weather data from satellites is part of the information provided. Many scientific disciplines and sectors of the U.S. economy have benefited from the applications of data from these satellites.

This information is a valuable asset and key resource for the Enterprise. As such, it is important to provide a secure, accurate, timely, reliable and cost-sensitive access to information that is critical to the Mission.

With the goal of improving information alignment and visibility across the Agency, there was a mandate for the development of a centralized Information Repository and Collaboration Tool. This was expected to improve coordination and planning across the various organizations within the Agency.

continued on page 4

> "The next time you look at the weather forecast, think about all the entities that work together seamlessly in the background to bring you the temperature in your neighborhood."