



Infrastructure Operations

Chad Wirz, VITA Service Delivery Manager

CIO Council Meeting
Sept. 12, 2012



- Chronic network issues program
 - Meeting with Verizon senior leadership – CIO Nixon
- Server monitoring
- Server patching
- Back-up monitoring
- Windows 7
- Review of issues and actions – Chad Wirz, VITA



Network Services Chronic Circuit (Site) Program

CIO Council Meeting
Sept. 12, 2012



NORTHROP GRUMMAN

Chronic Circuit (Site) Program

- Started in July 2009 during network transformation activities as a result of repeat repair tickets on MPLS/PIP circuits
- Goal – Identify sites which have recurring outages or are taking excessive circuit errors in an attempt to reduce or eliminate the reoccurrence of the problem
- Conduct daily site analysis to identify, isolate issues and determine next steps to resolve chronic outages to vendor, network customer premise equipment (CPE) or customer facilities; conduct weekly operational review meetings to discuss potential candidates for chronic site management



Chronic Circuit (Site) Program

- The Chronic Team, consisting of Northrop Grumman and Verizon personnel, track the circuits (site) on a log and perform daily health checks by logging into the router to review interface logs.
 - When issues are observed, after-hours stress testing is scheduled and conducted
 - Next step action(s) determined/taken based on test results
 - Sites are monitored seven to 14 business days following a hard fix action or up to 30 days if no issues are observed

Chronic Circuit (Site) Program

- There are two ways to get a circuit (site) into the program:
 - Proactive circuit analysis:
 - Data analysis, capacity reports, and vendor Web tool (eHealth), agency operations manager/customer initiated requests, Tier II incident management ticket, repeat service level agreement (SLA) failures
 - Incident management:
 - When an MPLS circuit has had three outages (Northrop Grumman: SEV 1 or 2, Vendor: Priority 1 within 30 calendar days
 - Executive management request

Chronic Circuit (Site) Program - Metrics

- Metrics are reviewed weekly by Verizon/Northrop Grumman operational team
 - To date, 217 circuits have been added to and cleared on the chronic program; five sites have cycled through the chronic program two times (2.3 percent)
 - There are currently two open active chronic circuits

Chronic Circuit Program - Verizon							
Month	Monthly Start Total	New	Moved Green	VzB Resolved	NG Resolved	Avg. Days to Green	Pri 1 Tickets
YTD AVG	6	5	5	4	2	32	7
Sept	2	0	0	0	0		0
Aug	11	3	12	8	4	28	7
July	5	13	7	5	2	27	23
Jun	3	4	2	2	0	31	3
May	9	2	7	6	1	52	4
Apr	7	3	1	0	1	30	7
Mar	3	6	2	1	1	43	3
Feb	4	3	4 (1 NTF)	3	0	31	3
Jan	6	3	4 (1 Blue)	4	0	23	2

Target Metric: Return To Green (RTG): ≤ 30 Day

Performance excellence driving low repeat rate of 2.3 percent

Chronic Circuit (Site) Program

- Conclusion
 - The program has corrected many issues proactively - preventing prolonged agency outages
 - Several chronic issues with sites have been isolated and resolved after years of complaints
 - Positive feedback received directly from agency contacts
 - Program demonstrates Northrop Grumman's and Verizon's commitment to continued improvements in network availability
- Follow-up
 - Program integration – Network operations
 - Agencies automatically engaged when site(s) added to program
 - Capacity management activities support chronic program

Questions?



HP OpenView Server Monitoring

Alvin Cajigas

CIO Council Meeting
Sept. 12, 2012



NORTHROP GRUMMAN

- **HP OpenView overview**

- Comprised of modules of software providing large-scale system and network management of our IT infrastructure
- Serves as a management solution that provides monitoring, reporting, troubleshooting and automated response capabilities necessary for delivering availability and service

- **HP Openview capabilities**

- Monitor up/down status
 - Interface availability response
 - Return to service validation
- Alerting to defined operating system/hardware characteristics to defined thresholds
 - CPU processing
 - Network
 - Memory
- End-to-end service management solution
 - Discover
 - Reaction trigger to events
 - Event tracking
 - Service levels

HP Openview monitoring configuration

– *Central processing unit (CPU) usage*

- Event - CPU exceeds set threshold for utilization
- Alert - Severity ticket created at 95 percent utilization for greater than two hours
- Action - Determine what services are using CPU and remediate where possible

– *Disk usage*

- Event - Disk threshold exceeded
- Alert - Severity ticket created at 95 percent (checkpoint at 0700, 1200, 1700 to minimize false alerts during backups)
- Action - Perform disk clean up on system drive and enlist agency help for data drives

HP Openview monitoring configuration

– *Physical memory*

- Event – Random access memory (RAM) usage threshold utilization
- Alert - Severity ticket created at 95 percent utilization for greater than two hours
- Action - Review if physical memory is available and what resources are over utilizing, recommend adding more where applicable

– *Page file*

- Event - Page file threshold near capacity
- Alert - Severity ticket created at 95 percent utilization for greater than two hours
- Action - Extend page file where applicable or move to subsequent drive as last resort

HP Openview Monitoring Configuration (continued)

– *Server interface connectivity*

- Event - Node temporarily fails to communicate with the server
- Alert - Severity ticket created if agent connectivity ping reply fails (validation is at five-minute intervals)
- Action - Generates incident after failed ping attempts; incidents are investigated immediately

Questions?



Server Patching

Alvin Cajigas

CIO Council Meeting
Sept. 12, 2012



- **Server patching**
 - Monthly patching cycles are security-centric in focus
 - The goal is to apply original equipment manufacturer (OEM)-released patches to the environment
 - IT infrastructure program security staff review and approve patches prior to release
 - Schedule verified and approved by agency authority

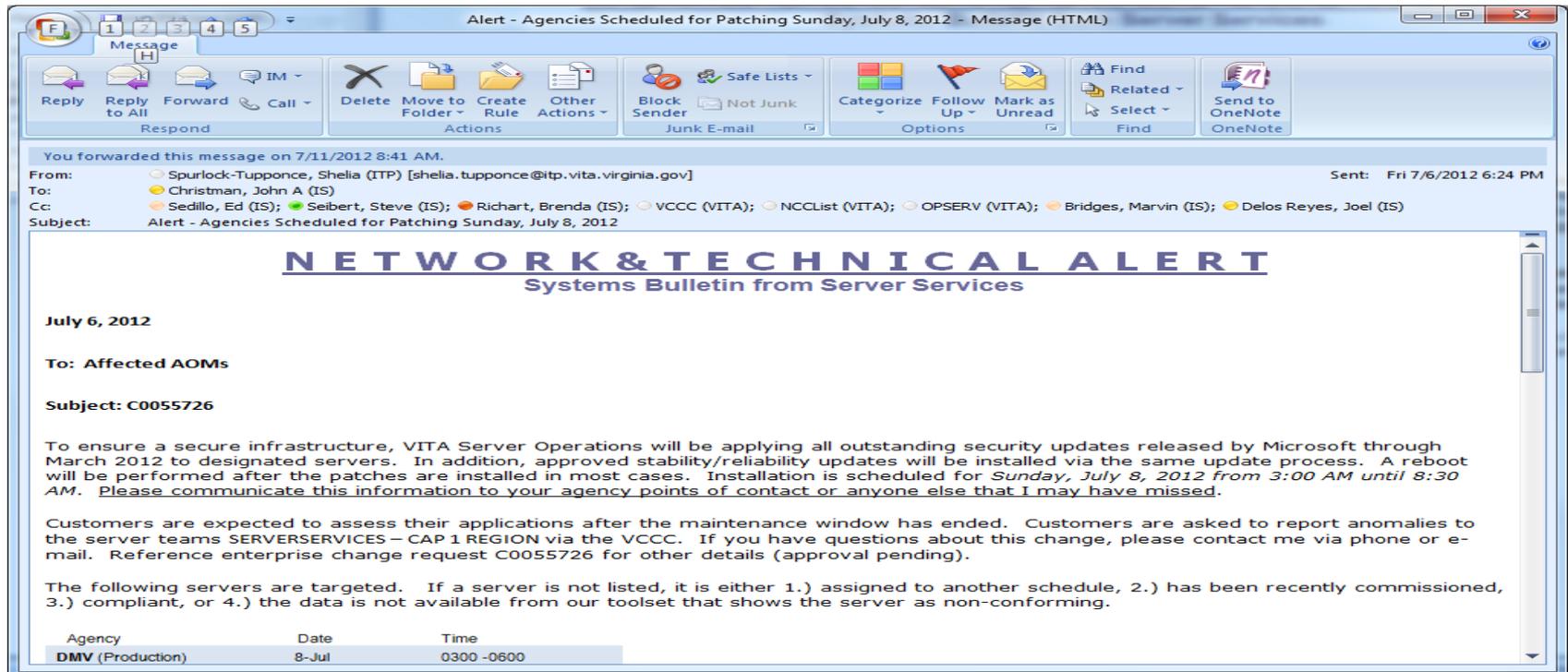
- **Patching process**

- The patching cycle is released to systems in a structured process as outlined below
 - Patches are released by Microsoft on second Tuesday of every month
 - Patches are reviewed by the security team to determine severity level
 - Final patch list released by the team by Friday at noon after patch Tuesday
 - Updates are staged by patch team and begin rolling out at 5 a.m. on Friday
 - Updates are pushed by Altiris to pilot servers, then production servers
 - All agencies are assigned specific days and times based on agency request

- **Patching communications**

- Agencies are notified of patching via the agency operations manager (AOM) communications

- Lists all servers that will be patched in a particular cycle as well as the number of patches expected
- Actual patch descriptions and severity ratings are published by the security team



Alert - Agencies Scheduled for Patching Sunday, July 8, 2012 - Message (HTML)

You forwarded this message on 7/11/2012 8:41 AM.

From: Spurlock-Tupponce, Shelia (ITP) [shelia.tupponce@itp.vita.virginia.gov]
 To: Christman, John A (IS)
 Cc: Sedillo, Ed (IS); Seibert, Steve (IS); Richart, Brenda (IS); VCCC (VITA); NCCLIST (VITA); OPSERV (VITA); Bridges, Marvin (IS); Delos Reyes, Joel (IS)
 Subject: Alert - Agencies Scheduled for Patching Sunday, July 8, 2012

Sent: Fri 7/6/2012 6:24 PM

NETWORK & TECHNICAL ALERT

Systems Bulletin from Server Services

July 6, 2012

To: Affected AOMs

Subject: C0055726

To ensure a secure infrastructure, VITA Server Operations will be applying all outstanding security updates released by Microsoft through March 2012 to designated servers. In addition, approved stability/reliability updates will be installed via the same update process. A reboot will be performed after the patches are installed in most cases. Installation is scheduled for *Sunday, July 8, 2012 from 3:00 AM until 8:30 AM*. Please communicate this information to your agency points of contact or anyone else that I may have missed.

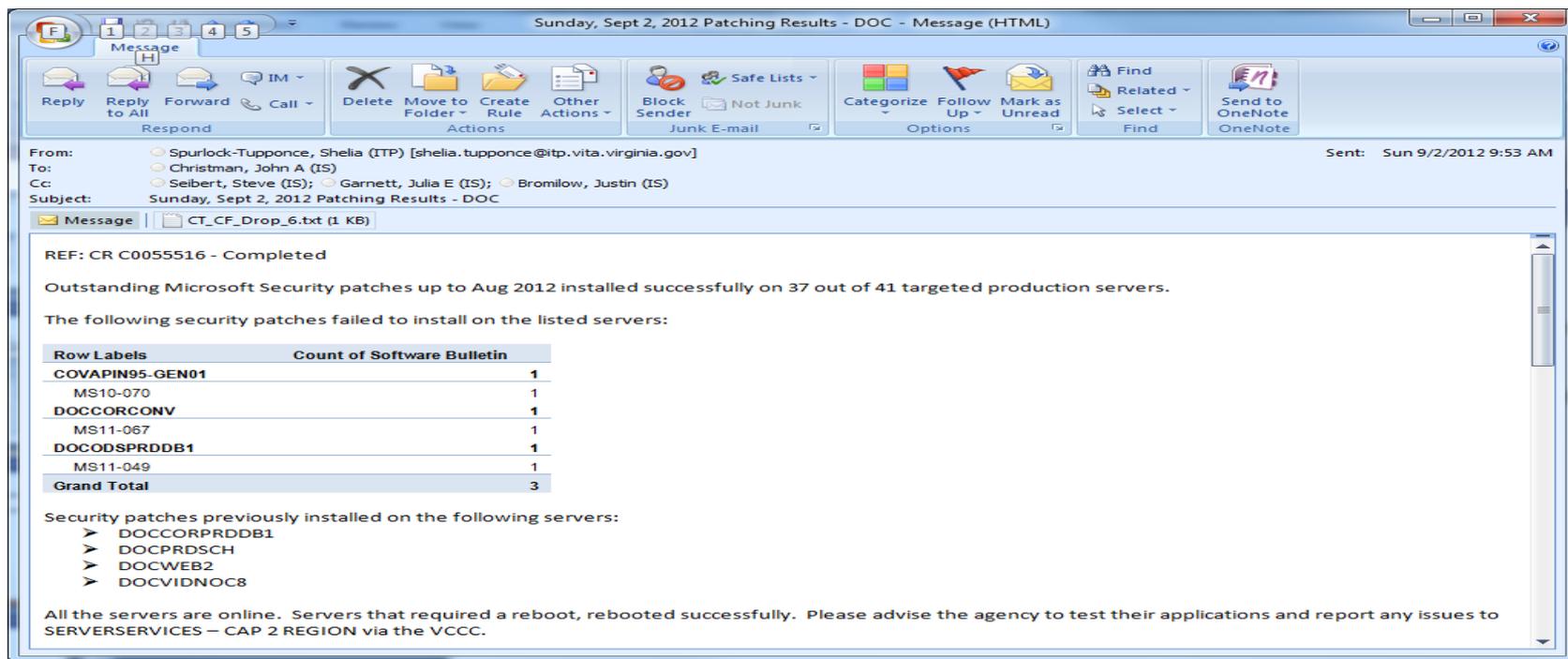
Customers are expected to assess their applications after the maintenance window has ended. Customers are asked to report anomalies to the server teams SERVERSERVICES – CAP 1 REGION via the VCCC. If you have questions about this change, please contact me via phone or e-mail. Reference enterprise change request C0055726 for other details (approval pending).

The following servers are targeted. If a server is not listed, it is either 1.) assigned to another schedule, 2.) has been recently commissioned, 3.) compliant, or 4.) the data is not available from our toolset that shows the server as non-conforming.

Agency	Date	Time
DMV (Production)	8-Jul	0300 -0600

• Patching verification and reporting

- There are specific steps in the procedure to ensure validation of patch completion and system availability after each patch cycle
- Followed up by close-out procedure steps and reporting of actions to agency authority
 - Patching considered OK only with good ping, good remote reboot time or task execution result
 - Upon completion of patching event, resolve change request, notify customer (via AOMs), notify Centralized Management Operations Center (CMOC) and on-call staff
 - Reports sent out to agencies within 24 hours of patching completion



Sunday, Sept 2, 2012 Patching Results - DOC - Message (HTML)

Message

Reply Reply to All Forward Call

Delete Move to Folder Create Rule Other Actions

Block Sender Not Junk Junk E-mail

Categorize Follow Up Mark as Unread

Find Related Select Find

Send to OneNote OneNote

From: Spurlock-Tupponce, Shelia (ITP) [shelia.tupponce@itp.vita.virginia.gov]
 To: Christman, John A (IS)
 Cc: Seibert, Steve (IS); Garnett, Julia E (IS); Bromilow, Justin (IS)
 Subject: Sunday, Sept 2, 2012 Patching Results - DOC

Sent: Sun 9/2/2012 9:53 AM

Message | CT_CF_Drop_6.txt (1 KB)

REF: CR C0055516 - Completed

Outstanding Microsoft Security patches up to Aug 2012 installed successfully on 37 out of 41 targeted production servers.

The following security patches failed to install on the listed servers:

Row Labels	Count of Software Bulletin
COVAPIN95-GEN01	1
MS10-070	1
DOCCORCONV	1
MS11-067	1
DOCODSPRDDB1	1
MS11-049	1
Grand Total	3

Security patches previously installed on the following servers:

- ▼ DOCCORPRDDB1
- ▼ DOCPRDSCH
- ▼ DOCWEB2
- ▼ DOCOVIDNOCB

All the servers are online. Servers that required a reboot, rebooted successfully. Please advise the agency to test their applications and report any issues to SERVERSERVICES – CAP 2 REGION via the VCCC.

Questions?



Server Backup Process

September 12, 2012



NORTHROP GRUMMAN

Backup Environment

- **Backup environment**
 - Enterprise backup consists of two environments: EBARS (Netbackup) and Avamar
 - Onsite backup environments –
 - VDOT – Netbackup and Tape Solution
 - DMV, DMME, VDH – Avamar grid at agency data centers
 - Daily backup reports
 - Daily EBARS and Avamar reports available and being distributed on a limited basis

Backup Environment

- **Backup and restore services include:**
 - Backups of local and storage area network (SAN) storage
 - Backups occur daily; includes one weekly full and six daily incremental - retained for 35 days
 - Monthly full backups are retained for 12 months
 - Backups offsite copy (SWESC or Iron Mountain)
 - Restore request service level agreements (SLA)
 - Servers at CESC/SWESC – restore must begin within four hours of ticket being opened
 - Servers not at CESC/SWESC – restore must begin within eight hours of ticket being opened

Backup Report

Client	Total Jobs	Successful	Failed	Active Jobs	Queued Jobs	% Successful (%)	Size (KB)	Num Files	Start Time	End Time	Agy_code
cddtsh01	9	9	0	0	0	100	31880192	438873	8/16/12 23:09	8/16/12 23:51	00501
cddtsh02	10	10	0	0	0	100	61065216	403214	8/16/12 23:09	8/17/12 00:05	00501
cddtsh03	7	7	0	0	0	100	46191616	426304	8/16/12 23:09	8/17/12 00:29	00501
cddtsh04	7	7	0	0	0	100	26941440	374205	8/16/12 23:09	8/16/12 23:40	00501
cddtsh05	9	9	0	0	0	100	16850944	395115	8/16/12 23:09	8/16/12 23:39	00501
cddtsh06	10	10	0	0	0	100	63356928	446724	8/16/12 23:10	8/17/12 00:17	00501
cddtsh07	9	9	0	0	0	100	5112832	160796	8/16/12 23:09	8/16/12 23:16	00501
cddtsh08	9	9	0	0	0	100	5068800	160481	8/16/12 22:59	8/16/12 23:10	00501
cddtsh09	13	13	0	0	0	100	746250240	970271	8/16/12 14:00	8/17/12 05:15	00501
cddtsh10	34	30	0	4	0	88.235	212683776	303106	8/16/12 22:59	8/17/12 10:46	00501
coapp27	2	1	0	1	0	50	0	0	8/16/12 21:00	8/16/12 22:46	00501
coextapp01	2	2	0	0	0	100	646144	457	8/16/12 17:30	8/16/12 23:48	00501
coextapp02	1	0	1	0	0	0	0	0	8/17/12 09:00	8/17/12 09:00	00501
coextapp03	2	2	0	0	0	100	4524032	832	8/16/12 17:30	8/16/12 21:05	00501

- **Color Key**
 - Green – Successful backup, Yellow – Backup in progress, Red – Failed backup of one or more jobs associated to that server
 - Orange – Job in queue, has not yet started
- **Server not listed in the report**
 - Backup job and was still running when this backup reporting day started
 - Server agency code incorrect, no job scheduled
- **Backup reports are generated daily between 9 a.m. and noon**
 - Contact your agency operations manager (AOM) to be added to the distribution list

Backup Remediation Process

- **Day 1**

- Backup team reviews backup reports
- Backup team works to determine root cause of backup failure
- Backup team implements corrective actions based on findings and opens tickets as required
- For backup failure, due to a single issue that impacts 25 or more servers, the backup team communicates to the AOMs the impact and path to resolution
- Backup jobs will be run the next night as scheduled

Backup Remediation Process

- **Day 2 and beyond**

- Backup team reviews backup reports to look for failures that have occurred two or more days in a row
- Repeat failures are documented using enterprise incident ticket and problem management system
- Backup team works to determine root cause of backup failure
- Backup team implements corrective actions based on findings
- For backup failure, due to a single issue that impacts 25 or more servers, the backup team communicates to the AOMs the impact and path to resolution
- Backup jobs will be run the next night as scheduled
- New report will be created to notify the AOM and agency of backup clients not backed up for EBARS for the last two days; AOMs can discuss with the agency criticality of the data and if they want to alter the backup schedule

Conclusion

- **Backup environment next steps**
 - Completion of agency server by server backup validation project
 - Upgrade of master media servers and software to version 7.5 to support growing capacity and keep technology current
 - Implement plan to move ~95 percent of the backup jobs to a disk-based solution, which will increase the backup success rate
 - Implement Avamar software to version 6.1 which will shorten the time it takes to perform data restore requests
 - Investigating if it is possible to create an automated report to pull all billable servers by agency and indicate which backups were successful for the previous night
 - Working towards an agency dedicated portal to view backup reports

Questions?



Windows 7

CIO Council
Sep 12, 2012



NORTHROP GRUMMAN

Windows 7 Deployment Status

- Project objective:
 - March 31, 2014: complete Windows 7 deployment
- Milestone: **Complete**
 - Conducted 68 of 68 agency Windows 7 application deep dives
- Milestones: **Past Due**
 - Sept. 4, 2012: complete load set approval
 - 36 agencies need to approve Windows 7 load set by Sept. 28
 - Sept. 4, 2012: approve Windows 7 deployment schedule
 - 36 agencies need to approve Windows 7 deployment schedule by Sept. 28

Accomplishments

1. **1,600 Windows 7 PCs in production**
2. PC refresh Windows 7 –**VMNH complete**
3. PC refresh Windows 7 -**VDH in progress**
4. PC refresh Windows 7 -**VDACS**
5. Windows 7 upgrade - **VITA in progress**
6. Windows 7 upgrade - **GOV in progress**
7. Windows 7 upgrade - **DCJS in progress**
8. Improved the printer setup process

Look ahead

1. Windows 7 application repackaging plan will be communicated in September
2. Anticipate eight agencies load set and schedule approval by Sept. 21
3. Identify and remove barriers to success for 25 agencies by Sept. 28
4. Finalize agency application remediation strategies for the following **Windows 7 at-risk agencies**
 - Three agencies at risk / 4,750 PCs to address: DGIF, DBHDS, VEC

Windows 7 Deployment Methods

- PC refresh – new hardware (23,000 PCs)
 - 32 agencies leveraging this approach
- In place “conversion” – existing hardware (30,000 PCs)
 - Centralized approach
 - Schedule specific dates and times for sites and users within a relatively narrow window of time; similar to the PC refresh process
 - **Local Approach**
 - **Provide a broad schedule, perhaps a month, for the user and a “local” end user services (EUS) technician to schedule and complete the upgrade**
 - Completed by EUS technicians
 - Schedule established by site

Require approval and input on local approach for Windows 7 deployment

Questions?

Review of Issues and Actions