One Policy to Rule them All

Efficiently Managing Impact Policies

Consolidated®
c o m m u n i c a t i o n s

Consolidated History

**Consolidated communications**

- **Consolidated Communications is a multi-state rural telecommunications service provider with a rich 100 year history.**

- **We currently provide and support:**
    - **Legacy Voice: 227,992**
    - **Voice over IP Telephone Services: 9,199**
    - **Commercial and Residential DSL: 110,913**
    - **IPTV: 34,356**
    - **Long-Haul Fiber Optic Transport**
    - **Metro Ethernet Services**

Consolidated Serving Areas

Consolidated Serving Areas

Network Operations Center
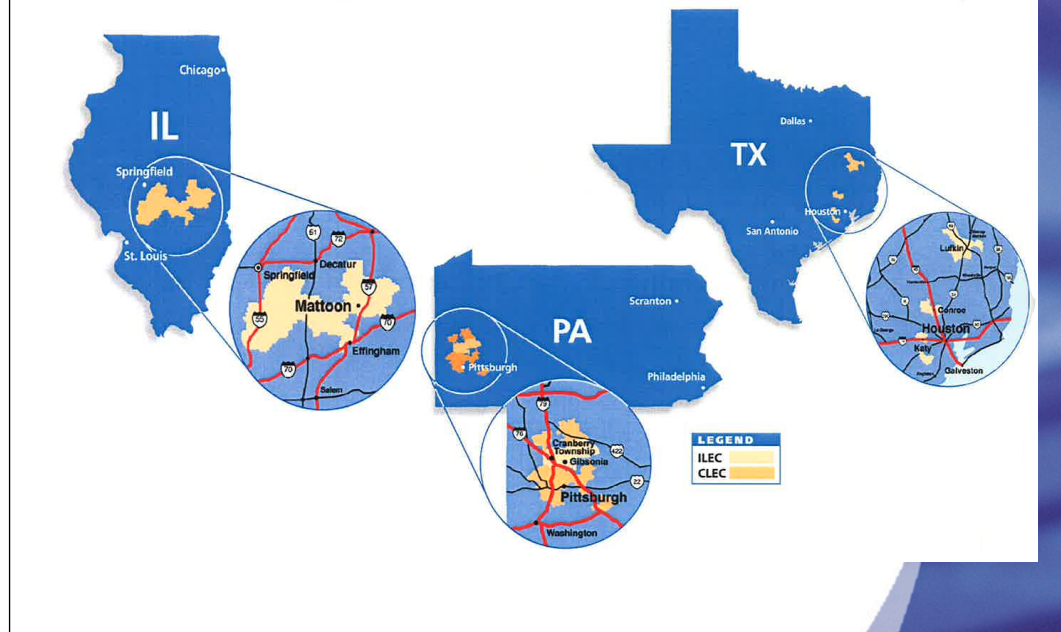
Consolidated communications
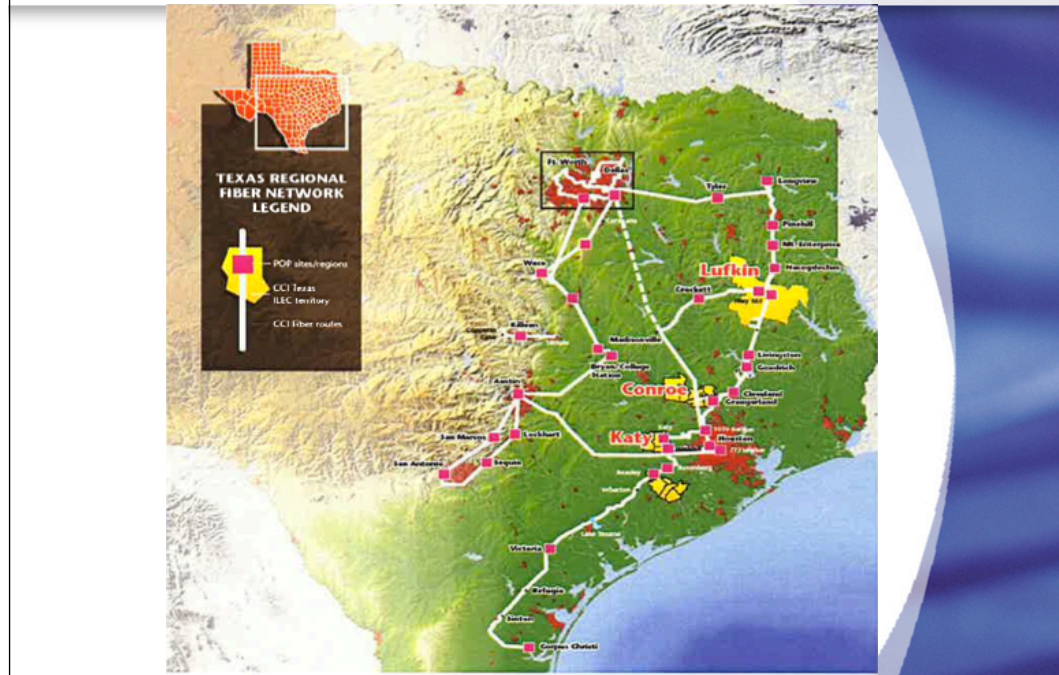
- **24x7 Operation**
- **Three states, each with multiple markets**
- **Multiple business units**
- **Responsible for**
  - **Infrastructure monitoring and response**
  - **Outage resolution**
  - **Customer notification**
  - **Vendor escalation and coordination**

Network Operations Center

- Tier 1 Network Facing
  - Respond to alarms/events
  - Resolve, dispatch or escalate
- Tier 1 Customer Facing
  - Respond to trouble tickets
  - Resolve, dispatch or escalate
- Tier 2
  - Provide escalated support
  - coordinate with vendors
- Tier 3
  - NOC Tools and Automation Team

Consolidated communications

NOC Tools and Automation Team

Consolidated communications

- **Maintain and manage IBM Tivoli Netcool Products**
- **Design and implement automation solutions to support the NOC and other Operations Units.**
- **Administer Servers and VMWare infrastructure for the Operational Business Unit.**

Work closely with the IT organization to retrieve operations specific data.
Intimate knowledge of java, scripting, sql etc..,

CCI's Business Challenge

Consolidated communications

- **Previous alarm monitoring solution was not flexible/scalable enough to support the NOC**
  - **Large number of scripts that required invocation manually.**
  - **Limited fields in database. No where to put enriched data.**

First Bullet.

- Myriad of scripts, various element managers invoked manually
- Desire to enrich events but only had one field to store enrichment data.
- Enriched data lost during lifecycle of event.

CCI's Business Challenge

- **Example Scripts/Policies**
  - **Environmental Monitoring Management**
  - **Enrichment:**
    - Circuits
    - Customer
    - Equipment
    - Geo-Data
  - **Operational Automation**
  - **Advanced Correlation Enrichment**
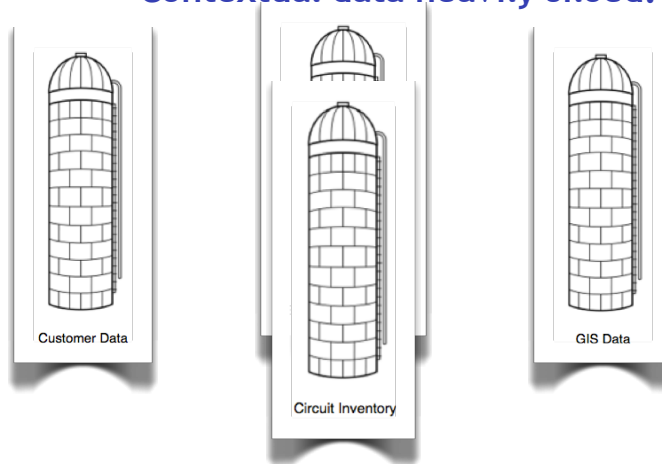
Just to give you an idea

-We had an initial need for quite a few policies enriching from multiple sources.

-Some policies would touch several sources in order to be fully enriched

-Notification of power failures

-X in Y DSP

Just to give you an idea

-We had an initial need for quite a few policies enriching from multiple sources.

-Some policies would touch several sources in order to be fully enriched

-Notification of power failures

-X in Y DSP

CCI's Business Challenge

Consolidated communications

- **Moved to Tivoli/Netcool Omnibus as event aggregator**

- **Selected Tivoli/Netcool Impact as enrichment and automation engine – the goal:**
  - *Centralize all our scripts*

- Many peers choose to use perl scripts instead of impact.

Simplistically: probes should parse, Impact should enrich.

Implementation Realizations

- **The need for a way to manage a large number of policies became apparent**

- **Multiple enrichment sources required based on type of event**

- **Events may require multiple policies to achieve full enrichment**

- **We can't add new ObjectServer fields every time we add an Impact Policy?!**

Evolutionary Note:

•We started moving our perl scripts and quickly determined it was going to be difficult to manage all of these scripts, we needed a better way.

- **One massive policy:**
  ◦ Difficult to manage in a team environment
  ◦ Single errors prevent entire policy from running
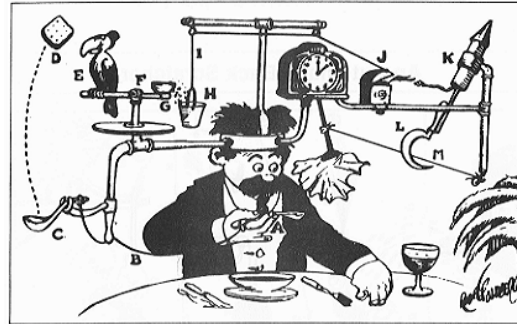
- One large policy containing all code or policy activations.
- Massively complex. In error in one section can prevent execution of the whole.
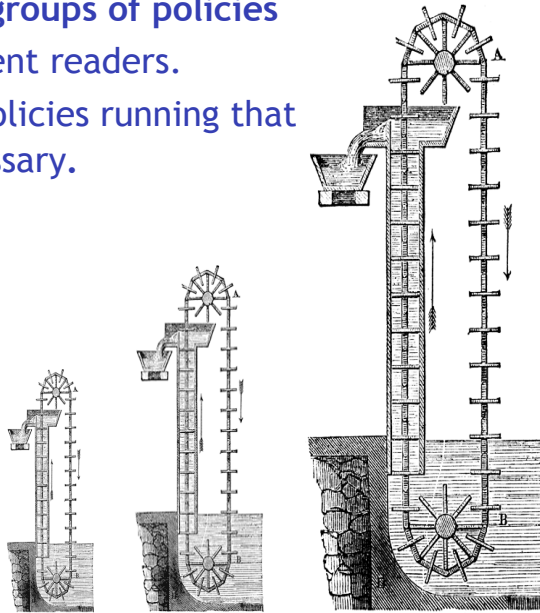- Difficult to develop new policies.

Methodologies

- **Chaining - all mappings:**
  - All policies run on all events
  - Unnecessary cycles
  - Where did enrichment fail?
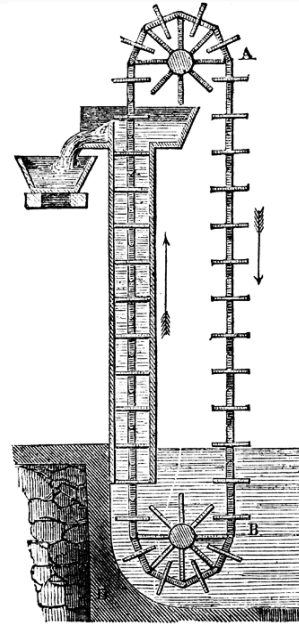
Little more modular, yet no error localization.

Possibly needless policy execution.

Methodologies

- **Chaining - groups of policies**
  - Multiple event readers.
  - Still have policies running that aren't necessary.

Step backward.

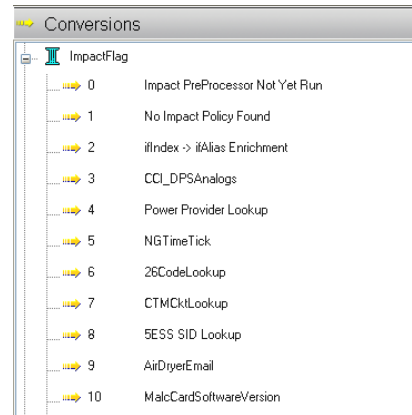All issues of previous just broken down into smaller segments.

Still no error localization.

Methodologies

- **Event Mapping**
- **Event Reader Mapping Restriction Filters only support SQL.**
  - Not enough granularity.
  - Complex mappings difficult

17

As the number of conditions increase per event, restriction filter becomes difficult to manage.

Derived Solution

- **Pre-Processor:**
  - Database Fields
    - One Impact Flag Field
      - Enumerated Values
      - Associated Conversion
    - One Impact Flag History Field
      - Contains history and status of every policy ran on an event.
  - Policies
    - One Parent Policy (Pre-Processor)
      - Based on defined criteria, assigns appropriate impact flag
  - Event Reader
    - Contains simple mappings based on impact flag

Database Fields

- **Impact Flag**
  ◦ Enumerated with Conversion

Database Fields

- **Impact History**
  - History "at a Glance"

| ImpactFlag	ImpactHistory	ImpactStatus	Node
MalcNumberOfCustomers	17-1,10-1,11-1,	1	DSLZON-CONRTXWVHX3-1006-040
BuildCLRUrl	17-2,12-1,13-1, 14-1,	1	LFKNTXXABB1
ifIndex -> ifAlias Enrichment	2-2(5),	2	CCITX-IDP
PassportCktLookup	12-3,	3	LFKNTXXABB2
BuildCLRUrl	12-1,13-1, 14-1,	1	LFKNTXXABB1
BroadSoftM6CustomerInf...	19-1,	1	SVRSUN-LFKNTXXA-CAB1301-25

Pre-Processor

- **All events are pre-processed**
- ◦ Impact Policy assignment based on:
  - ▪ SQL criteria
  - ▪ Match
  - ▪ Regmatch
- ◦ If { } elsif { } else
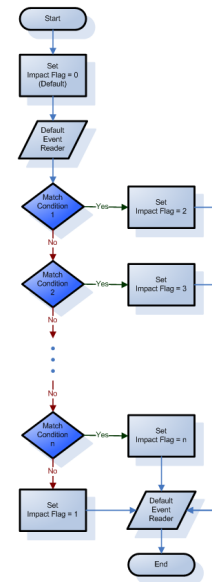
Pre-Processor

```
@ImpactStatus = 0;

Log("Started Impact Preprocessor... on Node: " + @Node + " " + @AlertGroup);

if (    (@AlertKey = "DEVICE_REACHABILITY_DOWN"
                or @Summary like "SYSB IDT"
                or @Summary like "Video Stream Outage"
                or @AlertGroup = "Softswitch State")
                and @Acknowledged = 0 ) {
                @Outage = 1;
                @Flash = 1;
                log("setting Outage and Flash to " + @Outage + ", " + @Flash);
} elseif ( @AlertGroup == "Generic Link Status" and (length(rextract(@Node, "(DSLZON)")) < 1)) {
                @ImpactFlag = 2;            .
} elseif ( Length(Rextract(@Summary,"(Verimatrix Digest Verification Failed)")) > 0 ) {
                Log("Spawn ClearVCASKey policy on " + @Node + " " + @AlertGroup);
                @ImpactFlag = 31;
} else {
        @ImpactFlag = 1;
}
if (@ImpactFlag == 0) {
    Log("Did not match any specified criteria");
}
ReturnEvent(EventContainer);
```

Event Reader

- **Simple Restriction Filters**
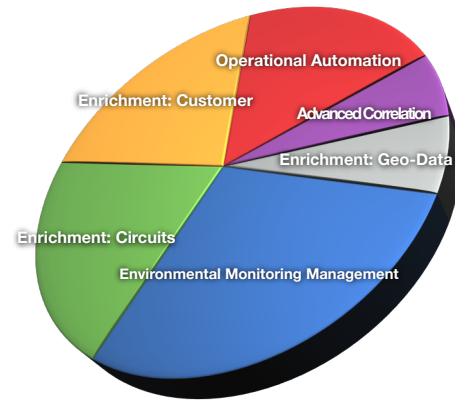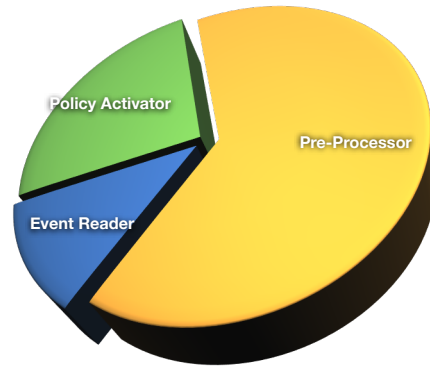
Operational Automation: Emailing groups, heartbeat monitoring.

Advanced Correlation: DSP's

Geo Data: Power Outage coordinates, Weather Warnings

Policy Management

- **Of the 33 active policies in use at CCI**
  - **20 are managed by the pre-processor**
    - **Reduces the number of event readers**

Pie chart with segments labeled: Policy Activator, Pre-Processor, Event Reader

Real World Applications

- **Decreasing Reaction Time**
- **Operational Automations**
- **Triple Play**

Real World Applications

Consolidated communications

- **Decreasing Reaction Time**
  - In policies that take corrective action, we have decreased the reaction time from hours to minutes - this is not the norm.
  - Raising priority of key events through policies decrease reaction time.
  - Error in a set top box encryption routine can cause a customer to be unable to rent Video on Demand. Impact takes action immediately rather than waiting for customer to call us with issue.

Impact Cost Benefit

- ## Corrective Action
  - ### Bug in set-top encryption routine
    - 1st level resolution estimated at $50/incident.
    - Approximately 6000 incidents until vendor provided a fix.

$300,000

$300,000

$225,000

$150,000

$75,000

Real World Applications
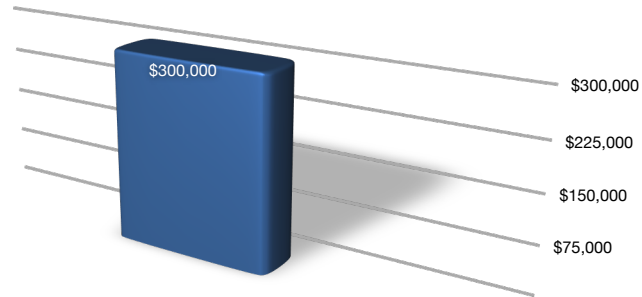
- **Average Information Gathering Time**
  - Enrichment Policies such as circuit lookup take 10 minutes on average, Impact does this in seconds.
  - Finding sub-rate circuits on a network link can take hours, Impact finds them and enriches alarms in seconds.

Impact History field enables cost benefit estimation.

Real World Applications

- **Operational Automations**
  - ○ Technicians spending a lot of time performing routine tasks as the result of an alarm.
    - updating databases
    - sending email notifications
  - ○ These tasks can be automated with impact.
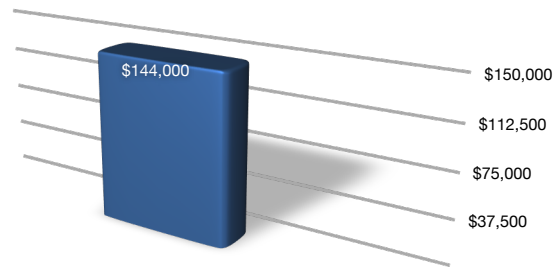
Operations had little confidence in the NOC to track exceptions.
80 generators, $150/per truck roll.

Real World Applications

- **Triple Play Monitoring**
  - **IPTV**
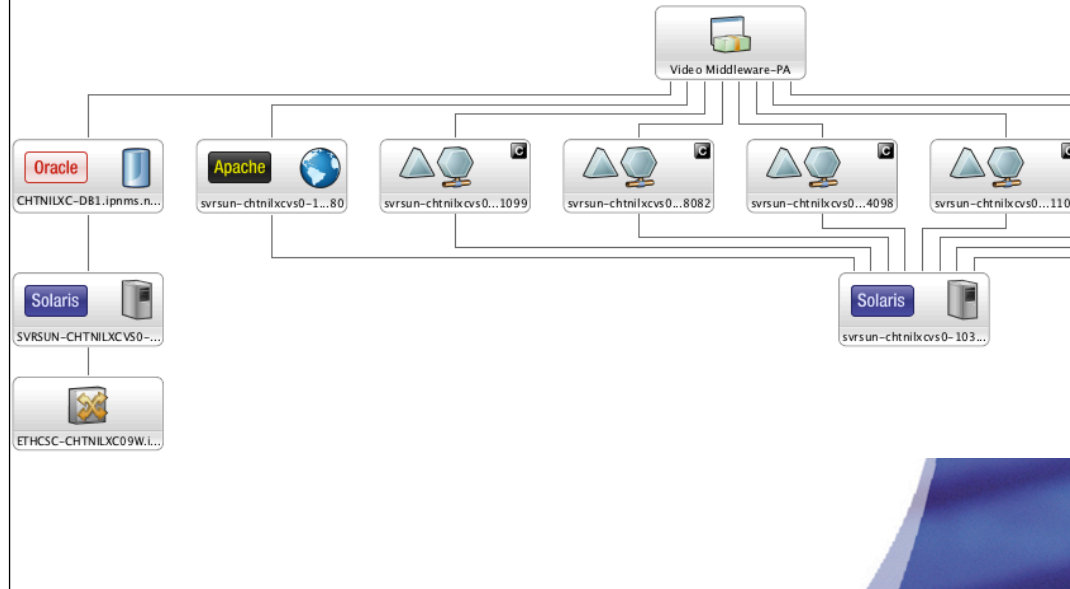   - Impact monitors Media Loss events, creating alarms in Netcool when thresholds are crossed.
    - Impact corrects settop encryption issues
  - **Legacy Voice/VOIP**
    - Trap and Trace is now normalized and platform agnostic.
    - Cable Theft Process automated.
  - **Internet**
    - Impact looks up interface details on every router/switch alarm. Internet uplinks increased in severity.

Your Environment…

- **How to extend this to your environment:**
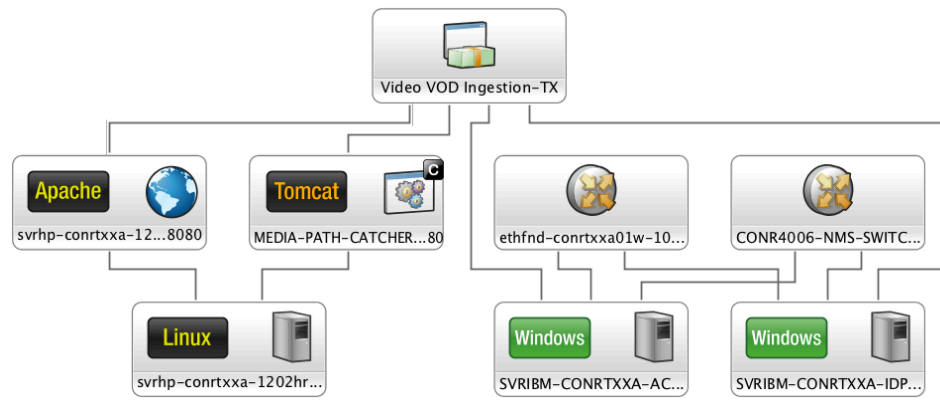 - Using built-in Netcool/Impact functionality customize this to your unique business context
    - Identify automation opportunities.
    - Identify sources of pertinent context
    - leverage impact to break down the silos
    - Track your own unique metrics for performance.
      - Enrichments/hour
      - Correlations/hour
      - Notifications/hour

Consolidated communications

Your Environment…

- **Remember the fundamental uses of Impact:**
  - To process high volume event streams to perform:
    - Enrichment: Gather additional information about an event
    - Suppression: Decide which events should be filtered out
    - Correlation: Set markers in diverse data sources
    - Auto-correction: Take action on devices (automations)
    - Notification: Alert staff about a high-priority condition
    - Escalation: If none of the above actions produced the desired results

Discovery/Modeling

CCI's Netcool Infrastructure

Consolidated communications

TBSM (2012)
Business & Service Modeling

InHouse Reporting Tools
Historical Reporting

Netcool GUI Foundation (NGF)
Common Application Server

Webtop
Web based event views

TADDM (in progress)
Application Discovery (Layer 4-7))

Gateways
Archive DB

3rd Party Trouble Ticketing

OMNIbus
Desktop
ObjectServer

Discovery & Monitoring

Impact
Advanced Correlation & Integration

DSAs

• Middleware
• Web Services
• Applications
• DBs
• etc...

ITNM (in progress)
Network Modeling (Layer 1/2/3)
Network Root Cause Analysis

3rd Party Performance Monitoring

Probes
• SNMP Traps
• Logs
• TCP Socket
• 3rd party APIs
• TEC
• etc...

3rd Party Monitors
• HTTP
• LDAP
• SAA
• TFTP
• TCP Port
• etc...

Events

Synthetic Transactions

Operations Infrastructure
• Devices
• Systems & Applications
• 3rd Party EMSs / Agents
• etc...

Efficiently Managing Impact

- **Questions**

Contact Info

- **Danny Butler**
  - danny.butler@consolidated.com
  - https://profiles.google.com/danny.butler
  - **Netcool Impact forum at IBM developerWorks**
  - **@deltabrav0**