UPLOGIX

Local Management Best Practices

SYNOPSIS | Immediately, and increasingly as new IT Infrastructure strategies such as virtualization and cloud computing lead to the increasing centralization of IT resources, management systems can and must be dramatically improved via the introduction of a Local Management component.

Local Management is not a single management discipline, but rather refers to the architectural strategy of enabling appropriate management tasks from across disciplines to be securely performed from a platform located with—and ideally directly connected to—select devices being managed.

The key to successful Local Management is knowing which management tasks to localize and which to perform centrally.

WWW.UPLOGIX.COM

What is Local Management?

Local Management is a network and systems management (NSM) practice that involves hosting a substantial management capability "locally" in the same location as the distributed infrastructure components that are being managed. The simple but transformational idea behind Local Management is to improve overall system cost effectiveness, performance, security and reliability by taking advantage of proximity.

Local Management is not a siloed management discipline but rather a new management approach that offers a better way to accomplish select management tasks from across disciplines. As such, Local Management is a critical component to be incorporated into existing management systems that will augment and improve them rather than replace them.

> "Local Management is not a siloed management discipline, but rather a new management approach that offers a better way to accomplish select management tasks. Local Management is a critical component to be incorporated into existing management systems that will augment and improve them…"

A locally deployed "Local Manager" is able to operate independently of the Wide Area Network, and when directly connected to managed devices using console or USB ports for access, can operate independently of the network entirely. This improves reliability and also removes network overhead as a management consideration while increasing the quantity and quality of information that can be collected. Other benefits of proximity and direct connection can include the following:

- The ability to more accurately monitor and simulate various user experiences from where the users are located
- More effective administrative security
- Out-of-Band remote access when networks fail and the ability to take a wider range of automated actions extending even to controlling power sources.

Ultimately this enables the lowering of operational expenses (or the ability to manage a growing increasingly complex environment without raising OPEX), increased capability to meet committed service levels and satisfy internal customers, and the elimination of security and regulatory compliance vulnerabilities.

There are benefits to be gained by locally managing network devices, servers, storage arrays and other infrastructure components, but not all kinds of infrastructure benefit equally. In-line network devices such as routers, switches and firewalls are typically the top priority for local management as without it, when these devices fail or experience problems, centralized management systems are rendered inert. When the network is up and running, the full power of centralized management tools can be applied to perform management tasks on other kinds of infrastructure components that might be required such as running scripts on or applying application changes to servers.

Some of the key defining attributes of a "Local Manager" include the following:

- **The ability to store large quantities of frequently updated device state and activity data, and to support rapid configuration rollbacks and changes.** This requires a sufficient storage capacity and appropriate storage medium to support a local transactional database to continually analyze network performance and interface statistics. This also requires sufficient capacity to store multiple configuration files, OS snapshots and logs from managed devices, as well as a fileserver capability (e.g. Xmodem, TFTP) to allow these things to be effectively utilized when needed by the Local Manager itself or by a technician accessing it.
- **The ability to take autonomous action** in response to managed device events or states or when instructed by an authorized administrator. This requires a robust-enough compute platform and an automation capability (rules engine) to locally execute complex tasks, processes and workflows specific to the devices to be managed.
- **The ability to securely connect to managed devices** with the same level of access (queries and commands) as an on-site technician would have (i.e. console port connection or equivalent).
- **The ability to integrate with centralized management tools** and be centrally controlled over the network when the network is available or when the network is unavailable to detect this and establish connectivity through alternate means autonomously.

The Increasingly Urgent Requirement for Local Management

Management systems have traditionally been centralized as this was believed to be the best approach for dealing with the challenges presented by the use of distributed heterogeneous computing platforms typical of client-server architectures.

Centralized Management for Distributed Systems

Client-server computing was initially adopted with the belief that decentralizing computing resources would improve the performance and scalability of business applications by eliminating large central servers and the network, both of which were very expensive, as performance bottlenecks. It also allowed IT departments to embrace and exploit the growing popularity of personal computers, which business users independently adopted for a variety of reasons including individual empowerment and flexibility.

While these expectations proved accurate in most cases, in the majority of cases serious management challenges quickly arose. Most of the challenges derived from the vast array of different kinds of servers, operating systems and personal computers that proliferated through the enterprise. Corporate IT was faced with having to manage environments with applications running across a very large number of geographically dispersed compute platforms with inconsistent and sometimes unique administrative interfaces and management requirements. The cost of management was staggering and service levels began to suffer with widespread adoption.

Systems management as we know it today was created to address the challenges of client-server once homegrown scripts proved inadequate. Tremendous investments have been made over the last 15+ years by organizations (and by the vendors trying to deliver them) attempting to gain efficient and reliable automated systems for managing these complex environments.

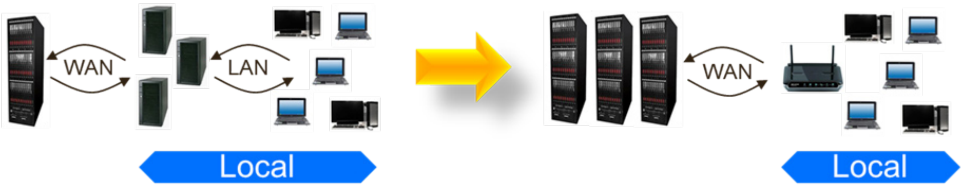
The approach taken was to install lightweight cross-platform management agents on managed devices and to develop a centralized management system that utilized the network to collect and organize information about the contents and state of the managed environment and that could perform management tasks over the network. Ultimately, with this approach sophisticated management systems made client-server a viable architectural approach for business. Still, problems persisted.

> “Ultimately, sophisticated management systems made client server a viable architectural approach for business. Still, problems persisted. The management systems and the processes organizations had to adopt to exploit them effectively became extremely complex in and of themselves.”

The management systems and the processes organizations had to adopt to exploit them effectively became extremely complex in and of themselves. The ultimate vision of highly automated administration has rarely if ever been realized due to this complexity. The ongoing management of client-server environments remains a major cost driver for most businesses and typically drives the large majority of costs incurred by IT departments. Enterprise Systems and Network Management technologies made the impossible merely very hard.

New Infrastructure Technologies Offer a Better Way

In recent years, two very important changes have rendered some of the underlying forces that drove enterprises to client-server architectures moot. First, virtualization and technological advances in CPU, memory and computer architecture allowed for low cost commodity computers to be used to perform tasks previously reserved for expensive specialized servers in a more efficient manner than ever envisioned. Second, network bandwidth has become both more available and considerably less expensive.



The role of the network, client-server versus virtualized infrastructures

Enterprises moving to capitalize on these developments are increasingly moving away from client-server architectures and toward a simpler, more manageable approach involving greater centralization of computing resources and applications accessed by users over the network with very little client or even mid-tier computing required. At the same time, the wholesale outsourcing of business applications to Application Service Providers (e.g. SalesForce.com) is becoming feasible. These providers can realize real economies of scale enabling them to offer enterprises cost savings and performance required by end users who are becoming more accustomed to network based applications.

Virtualization Creates New Management Challenges

As is often the case, the solution to yesterday's greatest challenges presents us with today's new challenges. As we move toward more easily managed and lower cost centralized infrastructures, we are dramatically increasing both our dependence on, utilization of and our sensitivity to issues with the network, both the WAN and the LAN.

For example with a typical client-server application, a WAN failure could potentially go unnoticed by end users for hours, or perhaps result in some temporarily reduced functionality, as users continue to work with their clients and their clients continue to interact over the LAN with mid-tier servers. With thin-client browser-based applications, network failures result in immediate and complete loss of functionality. Thin client architectures also typically send much more raw unprocessed data back and forth over the Internet for central processing, resulting in considerably more bandwidth utilization. Centrally managed networks will not be able to live up to these new more stringent performance and availability requirements.

> “... as the complexity of networks increases, visibility is increasingly becoming an issue. Overall, 35% of respondents indicated that their ability to troubleshoot network problems in a virtualized environment had worsened.”
>
> **Virtualization and the Cloud: The Trouble Is Troubleshooting**
> – Eric Savitz, Forbes ”

The Need for Local Management

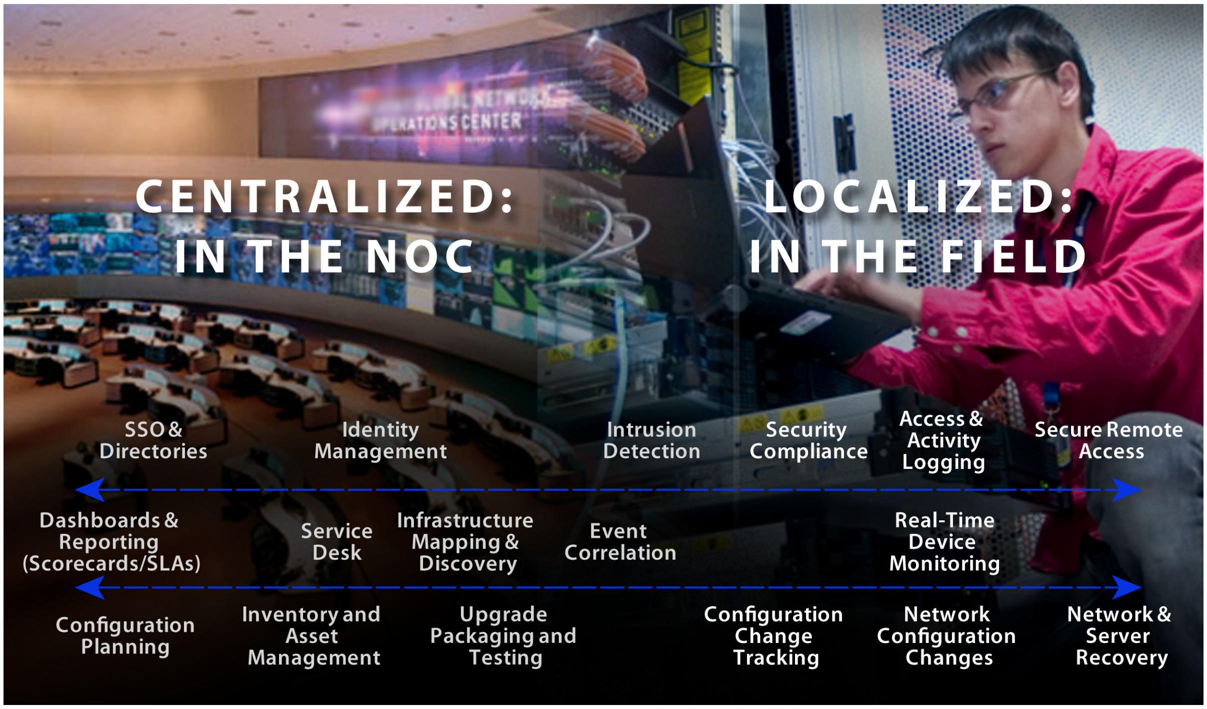
Systems management and especially network management approaches must adapt to remain effective. While somewhat counter-intuitive, as application platforms increasingly centralize and become accessed by users over the network, overly centralized network management approaches become problematic. Such approaches depend entirely on the network, which is already the critical overall point of failure in this new system, and while the computing infrastructure may be centralizing, network infrastructure, by definition, cannot.

The necessary response is to establish local management nodes that complement and augment existing centralized management systems to address the most significant vulnerability of the new computing model—network dependence and sensitivity. Any viable management system in the new architecture must have the ability to function independently of the network and bring a strong focus on ensuring better than previously acceptable network performance, availability and security. All while also automating potentially costly network management tasks. It needs to do this, including things like monitoring at intervals measured in seconds rather than minutes (something never feasible with centralized tools), without adversely impacting network performance.

> “The necessary response is to establish local management nodes that complement and augment existing centralized management systems to address the most significant vulnerability of the new computing model – network dependence and sensitivity.”

Best Practices – What to do Locally

The key to successful implementation of Local Management is selectively localizing the management tasks that benefit the most from it while maintaining centralized management where that makes more sense. Some decisions are obvious. Network topology visualization is necessarily a centralized task, out-of-band remote access is necessarily a localized task. Some tasks can be performed either way, depending on goals and priorities. However, it is easy to see that there are a set of management tasks where local is much better. A good rule of thumb is that whenever you have a routine maintenance task or upgrade where you would prefer to send a technician on site, it is probably a good candidate for automation via Local Management.


CENTRALIZED: IN THE NOC
LOCALIZED: IN THE FIELD
SSO & Directories
Identity Management
Intrusion Detection
Security Compliance
Access & Activity Logging
Secure Remote Access
Dashboards & Reporting (Scorecards/SLAs)
Service Desk
Infrastructure Mapping & Discovery
Event Correlation
Real-Time Device Monitoring
Configuration Planning
Inventory and Asset Management
Upgrade Packaging and Testing
Configuration Change Tracking
Network Configuration Changes
Network & Server Recovery

Management tasks divided based on whether they are best performed locally or centrally

The following Network Management tasks should be performed from a local platform, ideally directly connected to managed devices via their console ports.

Network Configuration and Change Management

Initial configuration

When a new network device such as a router or switch is installed, a significant amount of configuration work is required. Typically this is a manual task performed on site when centralized management systems are used, as a “bare metal” network device cannot be accessed over the network.

A Local Manager with console port level access can instantly detect when a bare metal (or otherwise improperly or incompletely configured) device is connected to it and automatically push a complete configuration to it. This greatly reduces manual labor and eliminates the opportunity for human error.

Executing configuration changes

Configuration changes ranging from updating ACLs to installing OS upgrades happen regularly. While the planning, testing and packaging of changes as well as enterprise reporting on the overall status and history of change projects is a task best performed centrally, the actual execution of changes is best performed locally. This is why NCCM tools are rarely used to automate changes.

The most significant argument for local execution is that changes are the most common cause of network outages. If changes are being made over the network and an outage occurs as a result of that change, no immediate corrective action can be taken by centralized management tools. A network-independent Local Manager on the other hand can be configured to apply changes, then automatically roll back configuration changes if issues occur using known valid states with very little risk.

This can have an impact on network operations that goes far beyond mitigating the occurrence and duration of outages vs. today. With this kind of comprehensive "safety net" less time needs to be spent on the arduous planning of changes in order to avoid possible errors. In addition, upgrades or configuration changes that deliver performance and functionality improvements can be more aggressively embraced and more administrative automation can be applied with confidence. This combines to extend the capacity and reach of IT personnel who know that if anything goes wrong, the network will be restored to an operating state very quickly.

> “This can have an impact on network operations that goes far beyond mitigating the occurrence and duration of outages vs. today. With this kind of comprehensive "safety net" less time needs to be spent on the arduous planning of changes in order to avoid possible errors. In addition, upgrades or configuration changes that deliver performance and functionality improvements can be more aggressively embraced and more administrative automation can be applied with confidence. This combines to extend the capacity and reach of IT personnel.”

Change tracking and audit

Security, regulatory compliance, fault resolution and performance optimization all require a crystal clear picture of the changes that have been made to a network device over time leading to the current state. This information needs to be available to central management tools, but should be captured and cached locally.

The primary reason for this is that sometimes the most difficult problems or sophisticated/sensitive changes call for on-site human attention and action. Having this information readily available on site and in detail for use by technicians empowers them to perform their work more rapidly, reliably and successfully. It is also usually necessary for compliance and always desirable for the purpose of diagnosis to have a system that can continue to securely document changes during network outages.

Network Performance and Availability

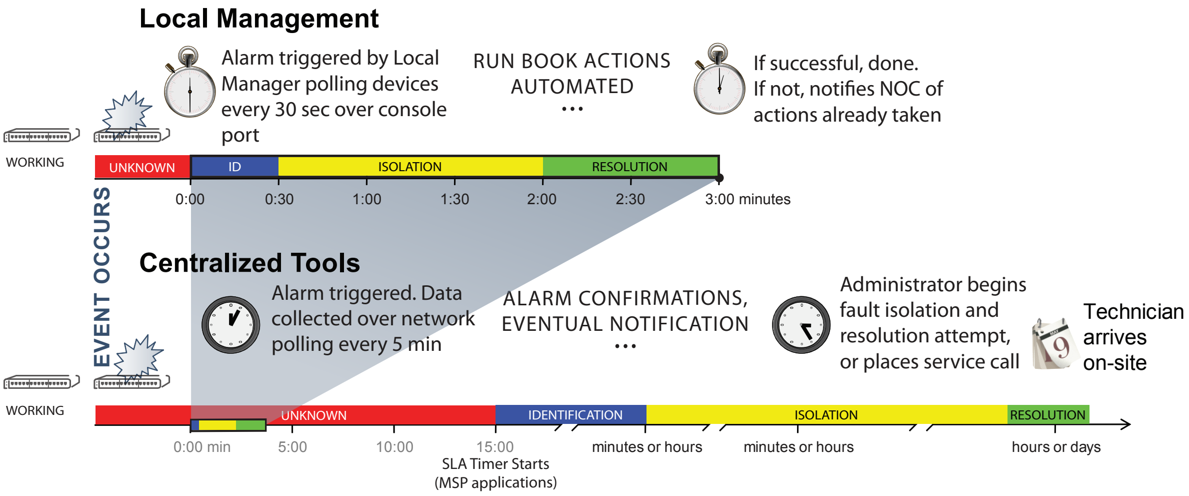
Device monitoring

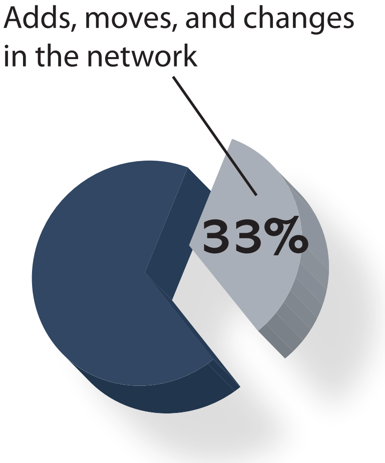
Monitoring the availability and performance of network devices is a basic requirement for meeting service level commitments. As infrastructures centralize this becomes more critical and the monitoring requirements become more stringent in response to inevitably more stringent network availability requirements.

Centralized monitoring approaches have always been vexed with the catch-22 that the act of monitoring network performance increasingly degrades network performance as it is done more intensively. This leads to compromises usually resulting in polling frequencies of around 5 to 15 minutes. As most processes don't identify a problem until two or three persistent problematic results are logged, this generally means that it can take 30 minutes or more before central systems even recognize that there is a problem requiring action. Even with these sacrifices in polling frequency, centralized management overhead on the network typically runs around an expensive 15% of capacity. None of this is likely to be acceptable to organizations utilizing centralized/cloud based thin client or ASP applications.

Device monitoring is one of the most beneficial applications of Local Management, because a Local Manager is not using the network to collect performance and availability data. Where a centralized tool may need to be restrained to 15 minute polling intervals, a Local Manager is typically configured to poll at 30 second intervals or less with no impact on the network. This combined with the use of automated problem resolution routines on a Local Manager means that with local management, problems can often be detected and completely resolved before central management tools would have even identified them.

> “Where a centralized tool may need to be restrained to 15 minute polling intervals, a Local Manager is typically configured to poll at 30 second intervals or less… with local management, problems can often be detected and completely resolved before central management tools would have even identified them.”


Local Management
Alarm triggered by Local Manager polling devices every 30 sec over console port
RUN BOOK ACTIONS AUTOMATED
...
If successful, done.
If not, notifies NOC of actions already taken
WORKING
UNKNOWN
ID
ISOLATION
RESOLUTION
0:00
0:30
1:00
1:30
2:00
2:30
3:00 minutes
EVENT OCCURS
Centralized Tools
Alarm triggered. Data collected over network polling every 5 min
ALARM CONFIRMATIONS, EVENTUAL NOTIFICATION
...
Administrator begins fault isolation and resolution attempt, or places service call
Technician arrives on-site
WORKING
UNKNOWN
IDENTIFICATION
ISOLATION
RESOLUTION
0:00 min
5:00
10:00
15:00
SLA Timer Starts
(MSP applications)
minutes or hours
minutes or hours
hours or days



QUESTION: "With respect to server virtualization, which of the following is your organization's biggest technical challenge?"

Server Virtualization Complicates Network Management
John Oltsik, Network World

Point to point user experience simulation

Network performance only matters as experienced by the end user. Centralized tools, by definition not located with end users, face limitations in measuring performance from this perspective. For example, a centralized tool can only synthesize a transaction over the network from the central location where it is installed to where the user is. It can also only synthesize a transaction over the network from the central location where it is installed to another location. It can never, however, synthesize a transaction between where the user is located and another specific location where it is not installed. Local management can add this dimension.

In this instance, the value of local management is derived from the opportunity for Local Managers to interact with one another. For example a Local Manager in one branch office could synthesize a voice over IP (VoIP) call to another branch office when both have Local Managers, measuring call quality and overall performance. This allows IT organizations to detect problems users are experiencing that might otherwise go unnoticed and to rapidly pinpoint problems in specific network segments when they are reported by end users.

One common example of Local Management in many organizations today is router hosted SLA measurement. Hosting a local simulation capability with the ability to make select router to router connections on the router (e.g. Cisco IOS IP SLA) delivers a dramatic improvement in visibility over centralized management approaches. Better yet is when the simulation, whether it is a VoIP, http or Ethernet transaction, is performed from a separate system connected to a router in the same manner as a user. This allow for issues that occur before a packet enters the router (e.g. improper quality of service policies) to also be detected.

Run book automation

A run book is a compilation of routine procedures that the administrator of a system carries out. Network run book automation is the defining, building, execution and reporting on automated workflows that support network operational processes based on all or part of this run book. A run book automated process can cross management disciplines and generally performs the same actions that an on-site technician would perform for a given set of circumstances.

The creation of the run book, the ongoing improvement of it and translation of all or part of it into automated routines is not something that innately benefits from localization, but run book automated execution benefits greatly. Most of the benefits derive from the fact that a Local Manager can automate a number of common and important actions typically found in network management run books that centralized systems cannot. This typically includes:

- Pushing an OS to and fully configuring a device without a working OS
- Performing a sequence of corrective actions when a device stops responding to polls (e.g. detect interface loss of signal, assess interface protocol state, clear service module, cycle the interface, show tech, reboot)
- Cycling power. This means effectively "unplugging" the device, or in the case of a Local Manager serially connected to an intelligent power strip, turning off the socket and turning it back on again.

Diagnostic trend capture

By grace of local presence and network independence, a Local Manager can perform frequent reliable sampling, store data such as snapshots locally for significant time periods so that they are not lost if a power cycle is required and initiate instantaneous queries in response to incidents even when the network is down as a result of the incident. This provides technicians with a wealth of diagnostic data to work with in resolving problems that would not be available with the use of fully centralized tools.

Network Security Management – Authentication and Authorization

The maintenance of administrative passwords and authorizations for network devices, to the extent that it is done, is typically done in network dependent systems like TACACS and RADIUS. Again, by grace of Local presence, a Local Manager integrated with such systems can maintain secure managed access during network outages. By caching passwords and authorizations from such centralized systems, a local management approach can completely eliminate the need for break glass passwords. Such passwords typically provide anonymous access and sweeping administrative privileges which creates a very serious security vulnerability.

> "By caching passwords and authorizations from such centralized systems, a local management approach can completely eliminate the need for break glass passwords."

Network Security Management - Auditing

Most industry compliance standards (SOX, PCI-DSS, GLBA, FSBA, HIPAA) and internal corporate standards have stringent requirements about auditing changes to the configurations of network devices as well as about limiting who can access them administratively and what information they can access while doing so. The reliance on centralized tools to do this can create significant vulnerabilities in two important ways.

First, auditing stops when the network is down. A Local Manager can continue to monitor and log all interactions with a network device regardless of the state of the network itself. With centralized solutions gaps are created during legitimate outages, and an opportunity for exploitation is created by anyone who has the ability to bring the network down and wishes to be able to access information make changes without leaving an audit trail.

Second, centralized tools generally rely on SNMP and Syslogs which are incomplete data sources. With a Local Manager directly connected to a network device, the opportunity is created to capture detailed sessions logs describing for example when a user logged on and off, which devices were accessed, commands run and the responses output by the device as a result of those commands.

Secure Out-of-Band Access

Out-of-band access is commonly provided by commodity console servers that connect to managed devices and include the basic ability to provide remote console access over a modem from anywhere an administrator needs access.

It is entirely possible to construct a Local Manager using a server connected to a Console Server with the Console Server providing the local management solution with the direct LAN-independent access it should have to deliver all of the potential benefits of Local Management. It is also possible to construct a Local Manager with RS-232 ports and a modem that can replace traditional console servers. In both cases the benefits of out-of-band access can be considerably improved vs. a console server-only based approach.

> “The key to successfully exploiting local management is to know which management tasks should be performed centrally and which management tasks should be performed locally. Once this has been successfully determined, some opportunities for beneficial interoperability become evident.”

While console servers are great time savers in many scenarios, they also create significant security issues. Console servers can be war-dialed. Further, Console Server traffic is rarely encrypted. With a Local Manager replacing or utilizing a Console Server, there is now enough intelligence to allow the Local Manager to detect a network outage and thereby know when it needs to dial out to establish a connection thus making it feasible to deactivate inbound connections. In addition, a more robust platform allows for the utilization of SSH encryption.

Local Management Working with Centralized Management

Local management is a way to augment and improve overall systems management functionality and reliability, thereby decreasing operational expenses, improving service levels and reducing security and regulatory compliance vulnerabilities. The key to successfully exploiting local management is to know which management tasks should be performed centrally and which management tasks should be performed locally. Once this has been successfully determined, some opportunities for beneficial interoperability become evident. Three integrations in particular provide exceptional value.

Out-of-band access for centralized management systems

A Local Manager can use its out-of-band connection to reconnect with centralized management systems. It can be set up to reconnect AAA systems like TACACS or RADIUS when the network goes down maintaining AAA integrity.

A Local Manager can also be set up to use its out-of-band connection to continue to feed critical information to centralized management consoles so that outages not immediately and automatically remediated by the Local Manager can be readily diagnosed.

Enriching data available to central consoles

Most centralized management systems have comprehensive and very powerful centralized reporting and analysis capabilities designed to allow IT administrators to make sense of problems in complex systems and to maintain an overall sense of the health of the operating environment. Local management can improve these systems by adding device state and performance data that can only be collected via direct console port connection, thereby augmenting the SNMP and Syslog data typically relied on by centralized consoles.

Safety net for NCCM systems

Modern centralized Network Configuration and Change Management Systems (NCCM) offer an array of capabilities for managing network devices including the ability to distribute software updates, make configuration changes, detect changes, establish and enforce compliance with network device configuration policies and report on network device configuration and changes across the enterprise.

However, when it comes to using such systems for executing changes, many organizations are rightly hesitant. Being network based, any changes that bring down the network will also render the NCCM system itself unable to address the problem.

Just the presence of a Local Manager can mitigate many of these concerns. The Local Manager will be able to detect any resulting outage and automatically execute the run book to attempt to remediate it. Additional benefits can be realized with a fairly light degree of integration between the NCCM system and the Local Manager. Two potential strategies would work. First, the NCCM system could notify the Local Manager of the incoming change at which point the Local Manager could pull the current working OS and configuration files. In the event of a detected outage, the Local Manager could restore the working configuration. A second approach could be to have the NCCM system deliver the change package to the Local Manager and have the Local Manager execute the change, taking advantage of the innate roll-back capability that is part of what any complete local management solution should provide.

Business Benefits of Local Management

When all of the capabilities that can take advantage of proximity are fully implemented, local management can reduce operational expenses (or allow for the management of growing environments without increasing them), improve service levels and improve security and regulatory compliance.

Reduce Operational Expenses

- Automate network device software upgrades and changes reliably
- Resolve problems quickly and with a minimum of manual effort when they arise
- Automate common maintenance tasks such as configuration changes and password resets.
- Reduce expensive site visits with automated problem resolution and out-of-band remote access
- Ensure the integrity of administrative logging which reduces the risk of regulatory compliance violations resulting in costly audits
- Reduce management traffic on the network

Improve Service Levels

- Monitor performance and availability much more intensively for much more rapid responses to issues
- Use Local Manager to Local Manager transactions to better monitor performance as experienced by end users
- Use locally hosted automation capabilities to take rapid action including a wider array of measures than possible with a network based approach
- Maintain central management console visibility into the state of local infrastructure when the network is down, facilitating appropriate and coordinated responses

Improve Security and Regulatory Compliance

- Enable more detailed auditing of administrative activities that are maintained whether or not the network is available
- Apply administrative security standards to network management by extending role based systems management policies to network devices
- Maintain administrative security policies when network connectivity is lost
- Eliminate the need for unaudited access to managed devices using "break glass" passwords with sweeping privileges
- Provide for remote access that cannot be war-dialed and that encrypts administrative interactions

Conclusions

Management systems have traditionally been centralized as this was a necessary first step for dealing with the highly distributed heterogeneous computing platforms typical of client server architectures. Now, due in part to the management and scalability challenges presented by Client/Server, computing architectures are evolving to a more centralized model.

Systems management approaches must adapt to remain effective and the necessary response is to establish local management nodes or "Local Managers" to address the most significant vulnerability of the new computing model – network dependence and sensitivity.

The key to success when developing, assembling or purchasing and implementing a local management solution is to focus on the management tasks that benefit the most from proximity. While local management can apply to a variety of infrastructure components, the highest impact area to focus on is network infrastructure to ensure network performance and availability as well as the ability for centralized management tools to reach servers, storage arrays and other infrastructure components.

The management tasks best suited to localization include the following:

- Select network configuration and change management tasks
  - Automating initial configuration of newly installed network devices
  - Executing configuration changes
  - Change tracking and auditing
- Select network performance and availability tasks
  - Device monitoring
  - Point to point user experience simulation
  - Run book automation (execution)
- Network security management - auditing
- Secure out-of-band access

When all of the capabilities that can take advantage of proximity are fully implemented, local management can reduce operational expenses (or allow for the management of growing environments without increasing them), improve service levels and improve security and regulatory compliance.

ABOUT UPLOGIX // **Uplogix provides the industry's first local management solution. Our co-located management platform automates routine administration, maintenance and recovery tasks—securely and regardless of network availability. In comparison, traditional network and systems management depends on the network, uses multiple tools, and remains labor intensive. Uplogix puts the power of your most trusted IT administrator everywhere, all the time.**

Uplogix is privately held and headquartered in Austin, Texas with international offices in London and Monterrey. For more information, please visit www.uplogix.com.

www.uplogix.com | Headquarters: 7600B N. Capital of Texas Hwy.
Suite 220, Austin, Texas 78731 | US Sales 877.857.7077,
International Sales +44(0)207 193 2769 © 2011 Uplogix, Inc. All rights reserved. *Uplogix*, the *Uplogix logo*, and *SurgicalRollback* are trademarks of Uplogix, Inc. All other marks referenced are those of their respective owners. 092311