Lotus knows.

Smarter software for a Smarter Planet.

Domino Server Monitoring

Zhi Qiang Sha(沙志强) | Manager, Lotus Notes/Domino, CDL

Agenda

- Server monitoring and analysis

- Domino Domain Monitoring

- Custom Monitoring and Third-Party Products

Server Analysis Overview

- Log.nsf
- Server Console
- Event Generators and Handlers
- Statistics Collection
- Activity Logging
- DCT
- DDM

Server Analysis Overview

- Admin client tab for server analysis shows
  - Log
  - Catalog
  - Administration Requests
  - Activity Trends
  - Domino Domain Monitoring
    - If you are not using it now, turn it on
      - Enable all of the probes
      - Let it run for the weekend
      - Turn them off if you're uncomfortable with letting it run
    - DDM finds problems before they cause crashes
      - Corrupt databases
      - "Bad" agents

IBM.

Server Monitoring

Domino Configuration Tuner(DCT)

- Easy to acquire, Easy to update, Easy to use
- Runs from your admin client
- Assess existing Domino deployments
- Requires no change to existing Server/Domain configuration
- Runs under/against Notes/Domino 7 and beyond
- Scans/evaluation can be initiated manually or scheduled
- Easy to expand rule catalog, frequently updated
- Rules are updated by IBM
  - New rules are pulled by you upon request
- Checks for low-hanging fruit in configurations
- Run it to help clean up an existing environment

IBM.

Domino Configuration Tuner(DCT)

DCT vs. DDM

- Domino Configuration Tuner (DCT) is a client based static analysis tool. DCT is great for detecting a wide variety of server configuration issues. It evaluates server settings according to a growing catalog of best practices.

- Domino Domain Monitoring (DDM) is a run-time server feature, DDM is great for detecting, understanding and acting on run time issues.

Agenda

- Server monitoring and analysis

- Domino Domain Monitoring (DDM)

- Custom Monitoring and Third-Party Products

Why Domino Domain Monitoring(DDM)

- *PainPoint 1*
- There is no tool can provide single view of the overall status of multiple servers across one or more Domains.

- *PainPoint 2*
- Administrators always spend much time to find out the cause when a server problem occur .

- *PainPoint 3*
- The analysis and fix of problem strongly depends on the experience and skill of Administrators.

What is Domino Domain Monitoring(DDM)

- First introduced in Domino 7.0

- A server based monitoring solution that provides to Administrators a *single* view of the overall status of multiple servers across domain

- Highly-*configurable* probes categorized by feature areas

- Default settings for easy *out-of-the-box* setup

- DDM automates problem determination and analysis in order *to reduce costs and time* associated with monitoring and troubleshooting your Domino environment

- Domino Administrators use the information provided by DDM to quickly *resolve issues before they cause more serious problems*

DDM Key Features

- *Active monitoring* capability: 58 new probes with highly-configurable schedules, content and targets.

- Domino domain monitoring data aggregation with *collection hierarchies*

- *Automatic problem determination* and determination of probable cause in multiple feature areas, and provide possible solution.

- *Delegation* of problems

- Automation of *corrective actions*

- *Auto-closing* for the resolved problem.

IBM.

Benefit from Domino Domain Monitoring

- Reduction in the Total Cost of Ownership by monitoring and troubleshooting servers and gathering the health of entire domain in a single UI/location

- Easy access to assessment and error reports

- Correlation capability for related problems

- Cross-server notification and reporting mechanism

- Corrective action context in many cases.

- Because efficient monitoring and problem resolution leads to
  - Server stability
  - Server uptime
  - Focus on business needs instead of the mechanics of administration

IBM.

log.nsf vs ddm.nsf

- **Domino generates errors and messages**
  - Error … "Object Store Manager: File does not exist"
  - Message … "Index update process started"
- **All logged errors and messages are raised as events**
- **Log.nsf records errors and messages sequentially**
  - Some messages are deliberately excluded because …
    - they are generated by printf debug spewage
    - an events4.nsf log filter configuration doc is defined
- **Log.nsf**
  - Pro: Great for maintaining a record of all errors and messages
  - Pro: Great for debugging, if you know what you are looking for
  - Con: Dumping ground for lost information

log.nsf vs ddm.nsf (Cont.)

- **As of Domino 7, all events are cached and tracked by DDM**

- **DDM.NSF is the on-disk version and superset of the event cache**

- **DDM.NSF records a <u>set of associated events</u> into a single report document (not just a single event)**
  - Pro: great for recording problem context
  - Pro: great for tracking and organizing problems
  - Pro: great for exposing knowledge about problems
  - Pro: great for resolving problems
  - Con: lousy for tracking sequential order of problems
  - Con: lousy for extracting ad hoc data from reports

The Components of DDM

Events	Events are generated by enabled probes, enabled Event generators and non-configurable embeddedprobes.
Probes	ProbesdothemajorityoftheworkandcanbeconfiguredtomonitorEventsinmultiplefeature areas(Replication,Security,andsoon).
Filter	FilterscontrolthevolumeofEventsthatappearinddm.nsf.Filtersareusedtospecifywhattype ofEventsshouldbeincludedintheDominodomainmonitordatabase.
Collection Hierarchy	One or more collection hierarchies can be created to roll up the Domino domain monitoring results(Event)informationintooneormorecollectionservers.
User Interfaces	MonitoringConfiguration(Events4.nsf)--usedtoconfigureDDMprobes,collection hierarchiesandfilters DominoDomainMonitor(ddm.nsf)--storesproberesults(Events)byseverity,date,andtype.

The Five C's of DDM

- Consolidate
  - Track multiple, related errors in a single event report
- Check
  - Assess health of functional areas
- Collect
  - Access all domain wide reports from a single database
- Correlate
  - Locate related reports from other servers
- Correct
  - Assess knowledge base of explanations and recommendations.
  - Click to resolve issues

The Five C's of DDM

- Consolidate
    - Track multiple, related errors in a single event report
- Check
- Collect
- Correlate
- Correct

Simple and Enhanced Events

- **Events can have one or two associated errors.**
- **When there are two errors, the "root cause" is the second error.**
  - 1 error: "Event: Could not locate view 'svrcollhier'"
  - 2 errors: "Object Store Manager: File does not exist"
- **Simple events are legacy events which include these attributes …**
  - Time stamp, originating server, resource strings and IDs, severities, types
- **Enhanced events also include the following attributes …**
  - New types, subtypes, target server
- **Enhanced events include one or more of these attributes …**
  - Target database, target user, target UNID, extra target data (i.e. string blobs), rich text, call stacks, correlation codes, and the NOTEID of a config doc responsible for firing the event.
  - This "target" data is some of the new event "context"

Event Reports

- **Like log.nsf, all events are recorded into ddm.nsf**

- **Unlike log.nsf, each set of events has it's own report document**

- **Each set of events has an associated unique ID (a PUID)**

- **Every event with the same PUID is mapped into the same ddm.nsf report document**

- **A PUID is built using the enhanced event context data**

  – Target database, target user, target agent, etc.

- **DDM.nsf Reports are presented in a variety of views,**

  as follows …

Event Report Views – Categorized

- **By Severity, By Date, By Type, By Server, By Assignment**

Event Report State

- **Open =** The event has a non-Normal severity and has not been manually closed
  - Auto Clearing Events = Some events can be automatically closed by DDM if the problem is reported as resolved with a Normal severity event
  - Many events must be closed manually
  - Simple events ever auto close (only enhanced events)
- **Closed =** The event has a Normal severity or has been manually closed
  - Automatically reopened if a severity change is detected
- **Permanently Closed =** Used by Admins to say "I don't care about this problem, keep it out of my sight."
  - Not automatically reopened, on a Normal severity, but continue to be tracked and recorded in its reports

Events Status Map

- Events statuses Map

DDM

Open

Administrator or
DDM (when a close
Event occurs again)

Administrator

Administrator or
an clearing Event

Administrator –
da verificare

Closed

Permanently Closed

Administrator (to monitor if an
Events will occur again)
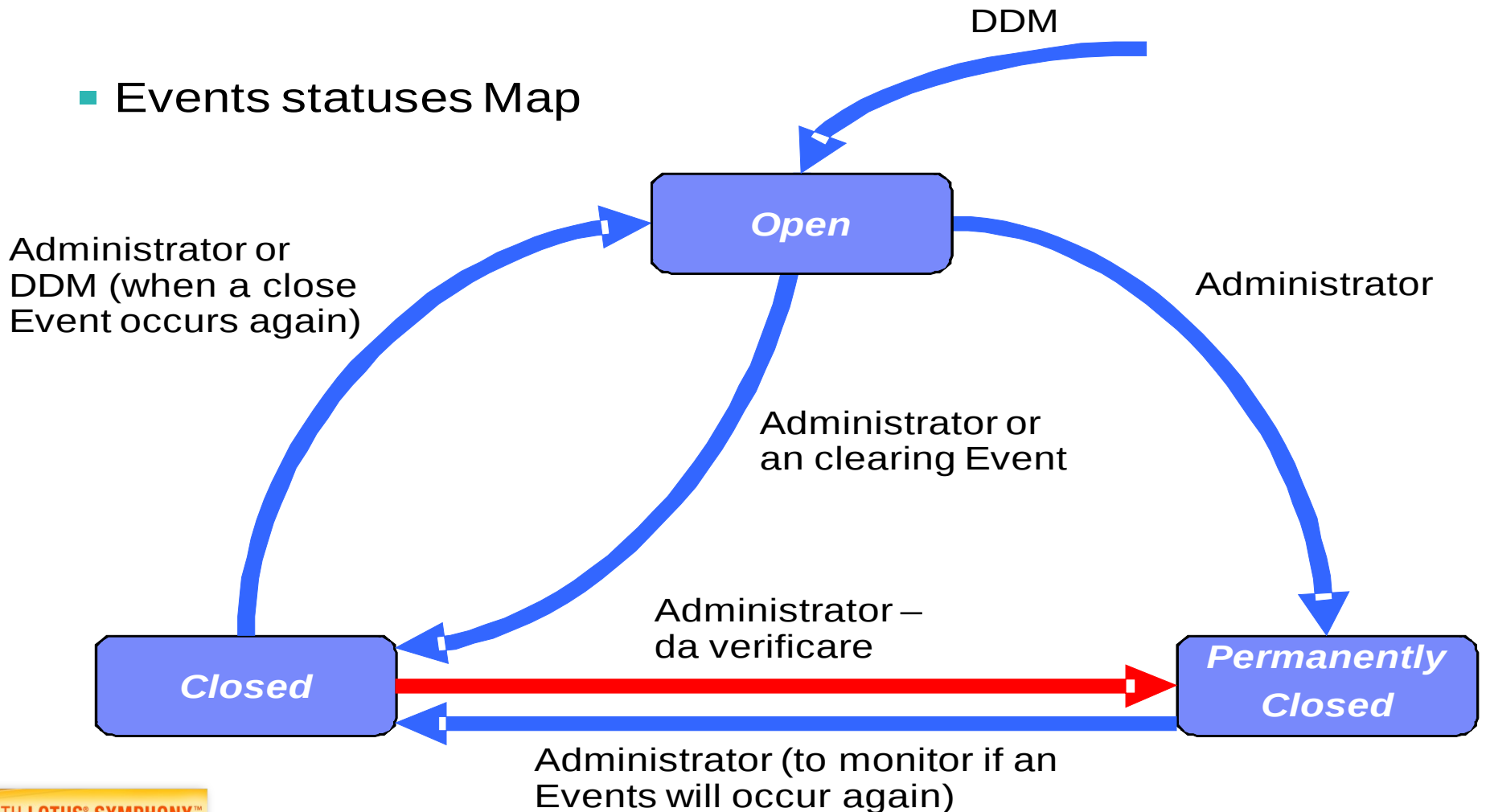
Event Report Views – Open, Recent, All

- **Open Events = All reports with a severity of non-Normal**

- **Recent Events = Actively Open or Closed in the past week**

- **All Events = Every Open, Closed or Permanently Closed report**

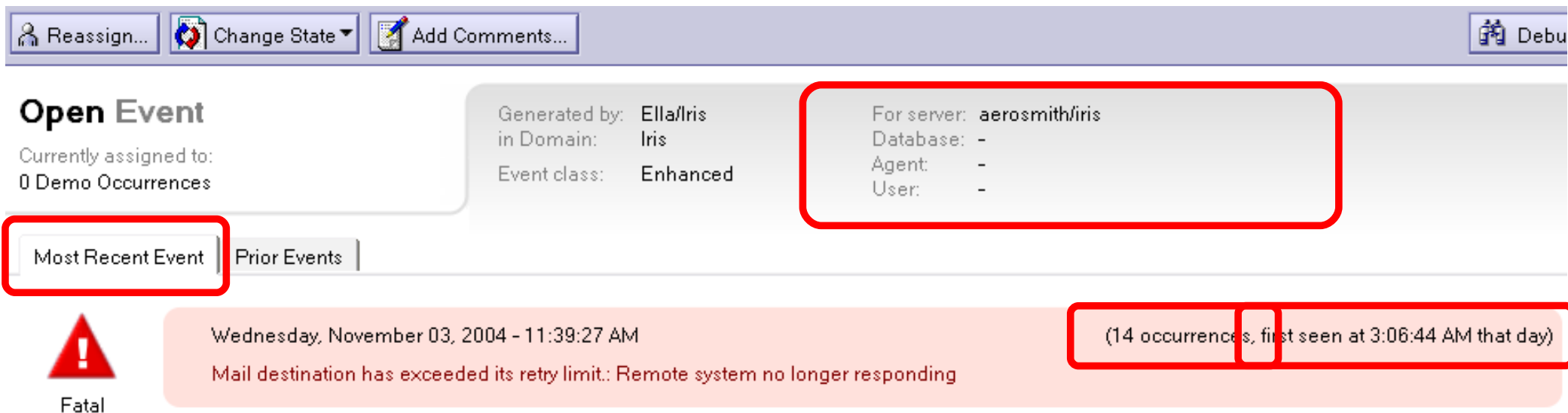# Event Report Basics

- **Comments, State & Assignment actions available in views and documents**

- **Originating server, Simple/Enhanced designation**

- **Available context data of enhanced events is highlighted**

- **The same error as that recorded in log.nsf**

- **With the same time stamp**

Event Report Occurrence Count

- **Additional occurrences of the same event are noted in the report**

- **The time of the first occurrence is recorded**

- **If you want the time of the in between occurrences ... search log.nsf**

- **Some enhanced events have less target information than others**

- **The current disposition for this error is the "Most Recent Event"**

Event Report Prior Events

- **When a new error maps into this report, but is not an exact match of the "Most Recent Event", instead of bumping the occurrence count ...**

  - The new error becomes the "Most Recent Event"

  - What had been the "Most Recent Event" gets pushed into the "Prior Event" list

This will happen because of a change of ...

- Severity

- Error text (new error)

- Error text (change to substituted parameter)

- ... and some others.

IBM.

Event Report Prior Events

- **At the bottom of the report is the Event change History.**

- **DEBUG_DDM=1 in the Notes client notes.ini will reveal some useful information about the report, like the PUID**

Event Change History:

04/19/2005 11:21 AM : John Paganetti/Westford/IBM – changed state to Permanently Closed
04/19/2005 11:21 AM : John Paganetti/Westford/IBM – added comments: Servers are out of Service
03/04/2005 11:50 AM : Chicks/Iris – changed state to Open

Developer debug information:

📄 CPU utilization no longer exceeds configured thresholds.

Template Version:	7.02		ACL level:	Manager (6)
Data Version:	3		ACL roles:	[Assign Events]; [Change State]
ConfigNoteID:	43BDA		Owner:	Yes
GeneratorNoteID:	0			
PUID:	Operating System/CPU CN=Brooks/O=Iris			

	Reason for change:	First occurrence in:	Latest occurrence in:	# Occ:	First occurrence:	Latest occurrence:	Latest Server.Time.Start:
1	Main Error	Release 7.0.1	Release 7.0.1	1	02/13/2006 04:47:01 AM	02/13/2006 04:47:01 AM	02/03/2006 13:36:46 EST
2	Main Severity	Release 7.0.1	Release 7.0.1	2	02/13/2006 04:34:01 AM	02/13/2006 04:44:01 AM	02/03/2006 13:36:46 EST
3	Main Error	Release 7.0.1	Release 7.0.1	1	02/13/2006 04:24:02 AM	02/13/2006 04:24:02 AM	02/03/2006 13:36:46 EST
4	Main Error	Release 7.0.1	Release 7.0.1	1	02/13/2006 03:36:02 AM	02/13/2006 03:36:02 AM	02/03/2006 13:36:46 EST
5	Main Error	Release 7.0.1	Release 7.0.1	2	02/13/2006 03:17:01 AM	02/13/2006 03:27:01 AM	02/03/2006 13:36:46 EST
6	Main Error	Release 7.0.1	Release 7.0.1	1	02/13/2006 03:07:02 AM	02/13/2006 03:07:02 AM	02/03/2006 13:36:46 EST
7	Main Severity	Release 7.0.1	Release 7.0.1	3	02/13/2006 02:39:01 AM	02/13/2006 02:59:01 AM	02/03/2006 13:36:46 EST
8	Main Severity	Release 7.0.1	Release 7.0.1	9	02/13/2006 01:09:02 AM	02/13/2006 02:29:02 AM	02/03/2006 13:36:46 EST
9	Main Severity	Release 7.0.1	Release 7.0.1	1	02/13/2006 12:59:01 AM	02/13/2006 12:59:01 AM	02/03/2006 13:36:46 EST
10	Main Severity	Release 7.0.1	Release 7.0.1	5	02/13/2006 12:09:02 AM	02/13/2006 12:49:02 AM	02/03/2006 13:36:46 EST

Consolidation into Event Reports, the bottom line ...

- Error states and the history of those states are organized into report documents

- Reports can be used as trouble tickets

- Reports include the contextual details about all the errors tracked by that document

The Five C's of DDM

- Consolidate
  - Track multiple, related errors in a single event report
- Check
  - Assess health of functional areas
- Collect
- Correlate
- Correct

DDM Probe Configuration

- **Events4.nsf – New DDM section**

- **DDM Probes / By Type**

- **Types are the major functional areas**

DDM Probe Configuration

- **Types expand into subtypes ...**

⊟ Application Code
- ⊞ Agents Behind Schedule
- ⊞ Agents Evaluated by CPU Usage
- ⊞ Agents Evaluated by Memory Usage
- ⊞ Long Running Agents

⊟ Database
- ⊞ Database Compact
- ⊞ Database Design
- ⊞ Database Error Monitoring
- ⊞ Scheduled Database Checks

⊟ Directory
- ⊞ Directory Availability
- ⊞ Directory Catalog Aggregation Schedule
- ⊞ Directory Catalog Creation
- ⊞ Directory Indexer Process State
- ⊞ LDAP Process State
- ⊞ LDAP Search Response
- ⊞ LDAP TCP Port Health
- ⊞ LDAP View Update Algorithm
- ⊞ Name Lookup Search Response
- ⊞ Secondary LDAP Search Response

⊟ Messaging
- ⊞ Mail DSN
- ⊞ Mail Flow Statistic Check
- ⊞ Mail Reflector
- ⊞ Message Retrieval Process State
- ⊞ Message Retrieval TCP Port Health
- ⊞ NRPC Routing Status
- ⊞ Router Process State
- ⊞ SMTP Process State
- ⊞ SMTP TCP Port Health
- ⊞ Transfer Queue Check

⊟ Operating System
- ⊞ CPU
- ⊞ Disk
- ⊞ Memory
- ⊞ Network

⊟ Replication
- ⊞ Replication Errors
- ⊞ Scheduled Replication Checks

⊟ Security
- ⊞ Security Best Practices
- ⊞ Security Configuration
- ⊞ Security Database ACL
- ⊞ Security Database Review
- ⊞ Security Review

⊟ Server
- ⊞ Administration

⊟ Web
- ⊞ Web Best Practices
- ⊞ Web Configuration

DDM Probe Configuration

- **Three flavors of probes (some probes have more than one):**
  - <u>Scheduled</u> probes run according to a configurable schedule and defaults are supplied
  - <u>Embedded</u> probes "instrument" the feature area and catch problems/issues as they occur
  - <u>Listening</u> probes run when particular error codes are logged

- **Probe configuration is quick and flexible:**
  - Defaults probe configuration documents supplied for "out-of-box" values
  - "Special target servers" concept allows out-of-the-box probing without having to specify named servers
  - Thresholds and result content are highly customizable
    - what the probe will actually check
    - probe sensitivity (when will they generate an event)
    - what severity event the probe will generate
  - Schedule is highly customizable for schedulable probes
  - Probes can be enabled/disabled per server/server group

DDM Probe Configuration

- **Default probe configuration documents ship with Domino 7**

- **These documents are initially disabled**

IBM.

DDM Probe Configuration

- **Default probe configuration documents ship with Domino 7**

- **These documents are initially disabled**

- **Probes can be enabled/disabled from the view ...**

DDM Probe Configuration

- **Probes can be enabled/disabled from the documents, as well**

- **The Basics tab always includes type, subtype & Description**

- **This Mail Reflector probe tracks mail sent to a particular address**

Save & Close ⊗ Disable Probe ⊗ Cancel

Messaging Probe: HPES-6FTQ5H

Basics | Schedule

Basics

Probe Type:	Messaging
Probe Subtype:	Mail Reflector
Probe Description:	『Demo Mail Reflector Probe』

This probe will test the mail flow to any mail system. To test mail flow to the destination mail domain, you will need to specify a mail recipient. The mail recipient must be configured such that messages received from this probe are sent back to the originator. The subject of the original message must be contained in the subject of the returned message. One way to configure this is to auto-forward messages from the mail recipient to the ISpy mail-in database on the server from which you are probing. *Note:* messages delivered by this probe to the mail recipient will not be automatically deleted from the mail file. You may want to specify a test user.

Target

Which servers should run this probe?
- ⦿ All Servers in the domain
- ○ Special Target Servers
- ○ Only the following servers:

- **All probe config docs include an explanation**

- **Specify the Target servers for any probe**

- **This probe will target (run on) all servers in the domain**
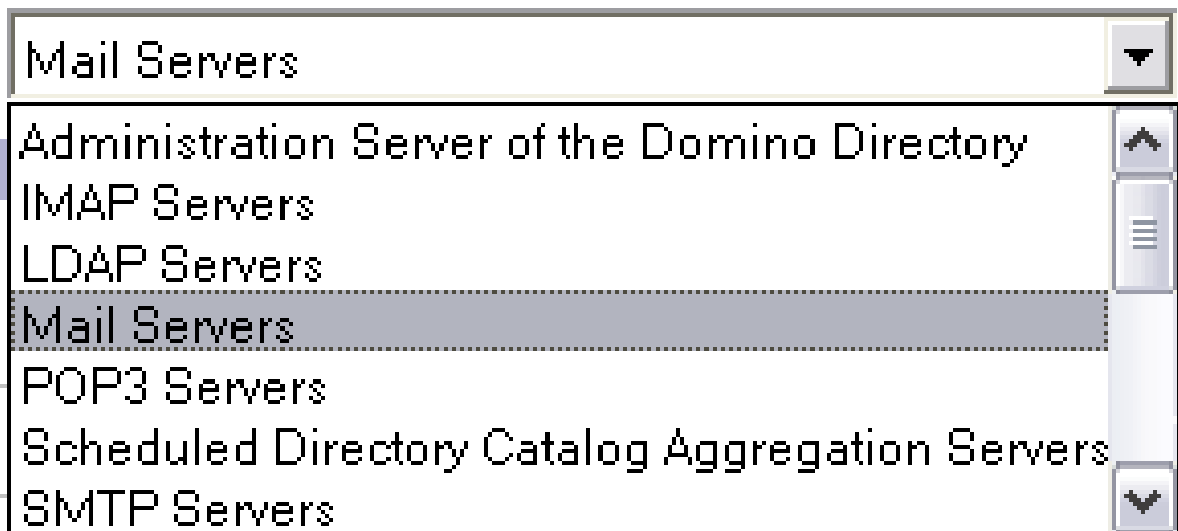
IBM.

DDM Probe Configuration

- **Select a Special Target Servers type so that you don't have to specifically name servers.**

  - DDM automatically figures out which servers are the Mail Servers

DDM Probe Configuration

- **Select a Special Target Server type so that you don't have to specifically name servers.**

  – DDM automatically figures out which servers are the Mail Servers
  – DDM automatically figures out other server types, depending on server tasks running and other configuration settings

Target

  – Special Target Server types allow you to configure probes without knowing
Which servers should run specific server names ahead of time. servers in the domain
this probe?

◉ Special Target Servers

○ Only the following servers:

Mail Servers ▼

Administration Server of the Domino Directory
IMAP Servers
LDAP Servers
Mail Servers
POP3 Servers
Scheduled Directory Catalog Aggregation Servers
SMTP Servers

Specifics

Mail Recipient:

☑ Enable   ⌐5⌐⌐ ⌐ seconds   Failure

DDM Probe Configuration

- **Depending on the probe, there are a variety of "specifics"**

Specifics

Mail Recipient:

michael peebles/music2

Specifics

Severity: Warning (high)   verity:

☑ Enable

Errors to ignore: | Basics | Specifics | Schedule |

☐ Enable

Specifics

☐ Enable   Which server settings should be validated?

☑ Compare Notes Public Key against those stored in directory   ☑ Check password

☑ Allow Anonymous Notes Connections   ☑ Required Change Interval

☑ Check passwords on Notes IDs   ☑ Check for existence of ID file in the person document

☑ Internet Authentication   ☑ Check the security of SSL Settings

☑ Check the security of Web Settings   ☑ Check the security of Domino Directory Settings

☑ Check the security of Mail Settings   ☑ Check the security of DIIOP settings

☑ Check the security of the Remote Debug Manager   ☑ Use more secure internet passwords

DDM Probe Configuration

- **Scheduled probe configuration documents have a schedule tab**

- **This Messaging / Mail Reflector probe can run every few minutes, 24/7**

- **Or, every few minutes, on specific days, in specific time windows**

- **Select which days the probe will run**

- **Select the time range when the probe will run**

Basics | Schedule |

Schedule

How often should this probe run?	⦿ Run multiple times per day
	○ Daily
	○ Weekly
	○ Monthly

Defined schedule: Every ⌜10⌟ minutes

Should this probe run twenty four hours per day, seven days per week?   ○ Yes ⦿ No

On which days should this probe run?
- ☐ Sunday
- ☑ Monday
- ☑ Tuesday
- ☑ Wednesday
- ☑ Thursday
- ☑ Friday
- ☐ Saturday

During which hours of the day should this probe run?   From 06:00 AM to 08:00 PM

DDM Probe Configuration

- **Some probes have the option to run as scheduled or in pseudo real time, like the Security / Best Practice probe**

- **Disable the "real time" mode to show scheduling options**

- **The schedule controls change to match Multiple, Daily, Weekly, Monthly selections**

- **For "Daily", select which days and at what time**

DDM Probe Configuration

- **Event Reports are generated because an error was logged**

- **Some of the logged errors are raised by enabled probes. The associated reports include a link back to the enabled probe.**

- **Event Generators (defined in events4.nsf) can also raise events. Reports created by an Event Generator will include a link back to that configuration document as well.**

Check health of functional areas, the bottom line ...

- **Actively look for problems**

- **Highly configurable and customizable**

- **Default configuration supplied out-of-the-box**

IBM.

The Five C's of DDM

- Consolidate
  - Track multiple, related errors in a single event report
- Check
  - Assess health of functional areas
- Collect
  - Access all domain wide reports from a single database
- Correlate
- Correct

Server Collection Hierarchy

- **Available from the DDM section in events4.nsf**
- **Create, delete or modify a hierarchy**
- **Select a hierarchy from the dropdown box**
- **Area51, the collecting server, includes reports from all of it's children servers**
- **Children servers include only their own reports**

Server Collection Hierarchy

- **Or click on an individual server to modify the hierarchy**
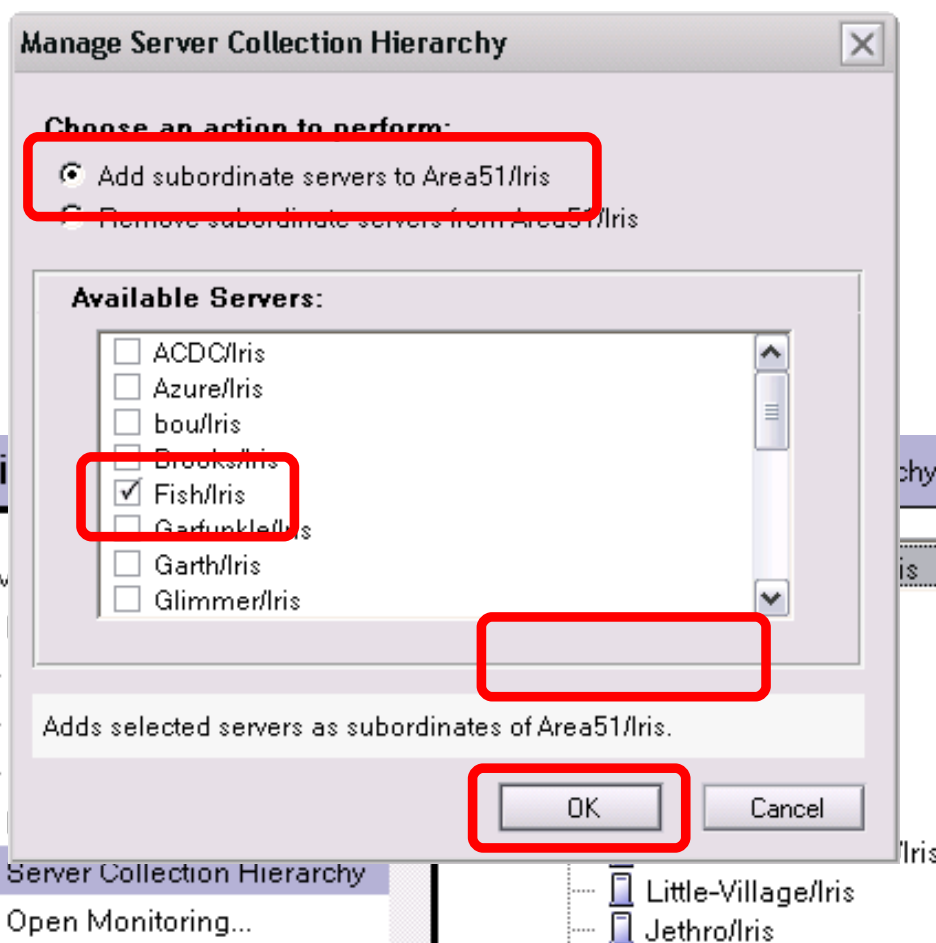
– Pick the action

– Select the servers

– OK
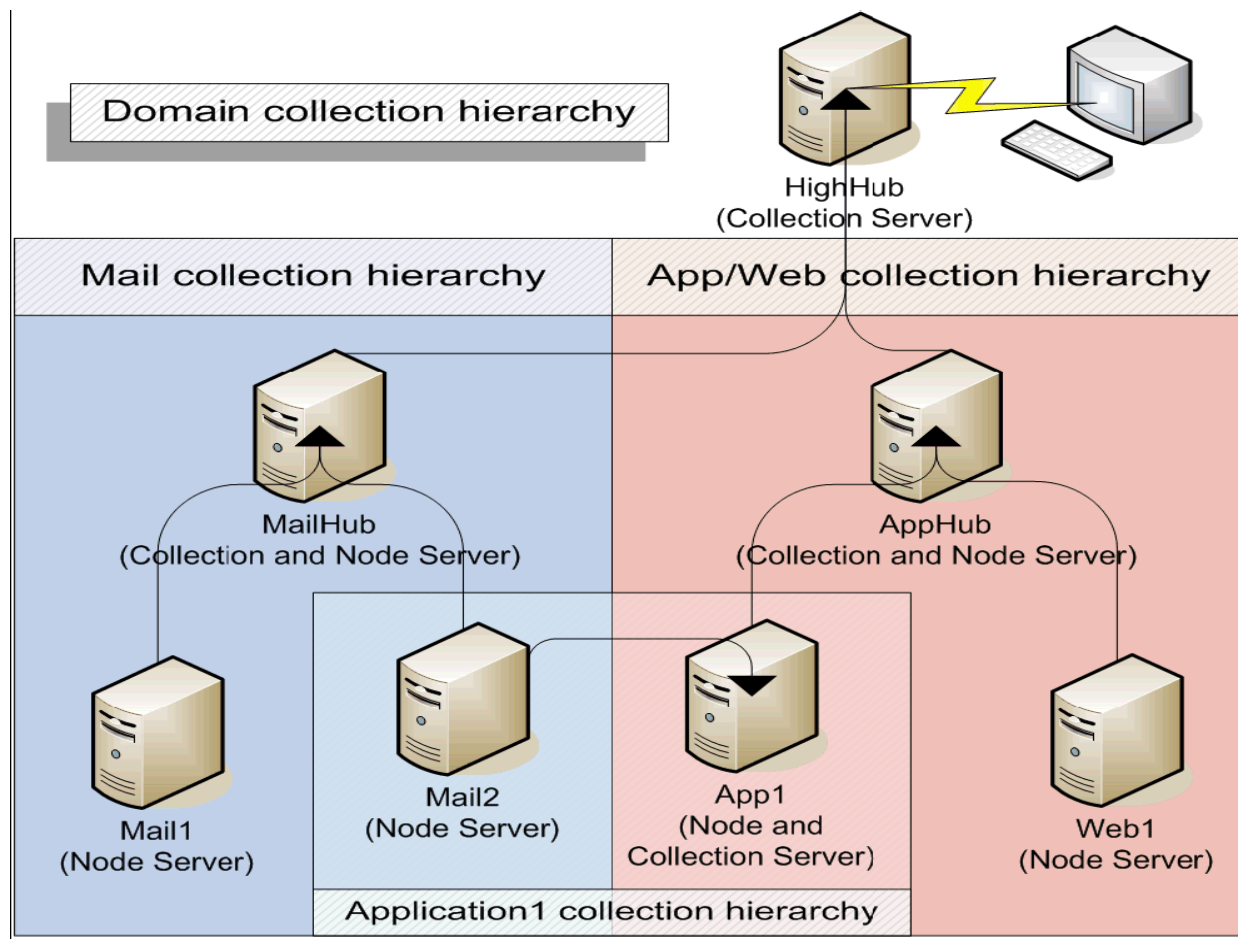
Server Collection Hierarchy

Server Collection Hierarchy

- **Servers generate report documents into their own ddm.nsf**
- **Reports are automatically replicated between the parents and children, as defined in the hierarchy**
- **Which documents show up on which replica of ddm.nsf is defined by the union of all server collection hierarchies in the domain**
- **The selective replication formula for each ddm.nsf is automatically defined and updated according to this hierarchy union**

Collection, the bottom line ...

- **Define hierarchies depending on what servers are of interest to particular Domino administrators**

- **Administrators can go to a single instance of ddm.nsf to work with every report of every server of interest**

- **Alternatively, administrators can open ddm.nsf on a leaf server of the hierarchy to see reports for only that server**

The Five C's of DDM

- Consolidate
  - Track multiple, related errors in a single event report
- Check
  - Assess health of functional areas
- Collect
  - Access all domain wide reports from a single database
- Correlate
  - Locate related reports from other servers
- Correct

Correlation

- **When there are multiple servers noticing the same problem, the report document will include a Correlated Events tab**

- **Select from this embedded view and take action on all these reports at once**

Correlation

- **Avoid confusion ...**
  - These buttons only work on the current document

  - These buttons operate on the documents selected in the embedded view

- **Prevent pain ...**
  - Never use <ctrl-a> in an embedded view because it will select <u>every doc in the parent view</u>, not just those currently displayed in the embedded view!

IBM.

Correlation, the bottom line ...

- **Some errors are noticed by multiple servers. Therefore, multiple reports are generated for the identical issues.**

- **Collection servers have replicas of all those multiple reports (if collecting from those reporting servers)**

- **Those identical reports are grouped together under the reports correlated tab**

- **Assign, Annotate or change the state of all the reports with at once**

The Five C's of DDM

- Consolidate
  - Track multiple, related errors in a single event report
- Check
  - Assess health of functional areas
- Collect
  - Access all domain wide reports from a single database
- Correlate
  - Locate related reports from other servers
- Correct
  - Assess knowledge base of explanations and recommendations.
  - Click to resolve issues

IBM.

Correction Leverages Knowledge

- **The Event Report explanation tab optionally has additional details about the error, like ...**
  - The link to the probe that caused the error to be generated
  - The Server task that generated the error
  - A link to the message document associated with the error (more on that in a minute)

Thursday, March 09, 2006 – 1:13:41 AM   (2 occurrences, first seen at Wednesday, March 08, 2006 – 1:13:40 AM)

Agent Manager: 12 minute(s) have elapsed since start of agent 'OutOfOffice|OutOfOffice' in database 'mail\MMcGover.nsf'. Threshold level 10 minute(s). Agent Owner: 'Martha McGovern/Westford/IBM'.

Explanation

- Triggered by:
- Reported by: Agent Manager
- Severity and type: ⚠ Fatal in Application Code
- Probable cause: An agent is running longer than the threshold specified in the probe configuration.
- Possible solution: 1. Cancel the agent 'OutOfOffice|OutOfOffice' in database 'mail\MMcGover.nsf' on server 'Chicks/Iris' from the server console or from the Administrator Client using "tell amgr cancel "mail\MMcGover.nsf" 'OutOfOffice|OutOfOffice' " console command. (Agent Manager agents only)
                        2. Examine agent performance by profiling it. To enable profiling edit the agent and then select 'Profile this agent' option on the second tab of the agent's properties. The next time this agent will run it will generate profile information which can be viewed from Designer's Agent menu by selecting 'View profile results'
                        3. Send a message to the agent owner 'Martha McGovern/Westford/IBM'
- Corrective action: [Choose Solution...]

Correction Leverages Knowledge

- **Probable cause = 0, 1 or more reasons why this might have happened**
- **Possible solution = 0, 1 or actions that might resolve the situation**
- **Corrective action = 0, 1 or more clickable resolutions or helper actions**

Thursday, March 09, 2006 – 1:13:41 AM   (2 occurrences, first seen at Wednesday, March 08, 2006 – 1:13:40 AM)

Agent Manager: 12 minute(s) have elapsed since start of agent 'OutOfOffice|OutOfOffice' in database 'mail\MMcGover.nsf'. Threshold level 10 minute(s). Agent Owner: 'Martha McGovern/Westford/IBM'.

| Explanation |

- Triggered by:
- Reported by: Agent Manager
- Severity and type: ⚠ Fatal in Application Code
- Probable cause: An agent is running longer than the threshold specified in the probe configuration.
- Possible solution: 1. Cancel the agent 'OutOfOffice|OutOfOffice' in database 'mail\MMcGover.nsf' on server 'Chicks/Iris' from the server console or from the Administrator Client using "tell amgr cancel "mail\MMcGover.nsf" 'OutOfOffice|OutOfOffice' " console command. (Agent Manager agents only)
2. Examine agent performance by profiling it. To enable profiling edit the agent and then select 'Profile this agent' option on the second tab of the agent's properties. The next time this agent will run it will generate profile information which can be viewed from Designer's Agent menu by selecting 'View profile results'
3. Send a message to the agent owner 'Martha McGovern/Westford/IBM'
- Corrective action: Choose Solution...

Correction Leverages Knowledge

- **Probable cause = 0, 1 or more reasons why this might have happened**
- **Possible solution = 0, 1 or actions that might resolve the situation**
- **Corrective action = 0, 1 or more clickable resolutions or helper actions**
  - There may be multiple choices under a single button. The number of corrective action choices may not match the number of possible solutions offered.

Correction Leverages Knowledge

- **Some event reports include two errors. The second one being the 'root cause'.**
- **Sometimes both errors have associated cause, solution and action information**

Correction Leverages Knowledge

- **The knowledge database is the collection of message documents in events4.nsf**

- **The Severity and type, Probable cause, Possible solution and Corrective action for this error is stored in a single message document**

- **Follow the link to examine or modify that document**

- **(Of course, message config docs are accessible from events4.nsf views, too)**

Knowledge Defined in Message Documents

- **Since we're looking at message docs, let's cover the entire thing ...**
- **Customers are encouraged to change Severity and Suppression time, if necessary**
  - Future instances of this error will have the new severity (existing history is not changed)
  - Suppression will prevent alarms from being trigged by multiple occurrences of this error for the specified period of time. (Alarms have been around for many releases)

Basics | Probable Cause/Possible Solution | Corrective Action(s)

Original text:	Warning: Cannot locate design note '<string>' in '<string>' template
Addin name:	
Value:	0x300D
Event type:	Database
Event subtype:	Design
Old Event type:	Misc
Event severity:	Warning (high)
Suppression time:	0 minutes
Event correlation:	Server and Database wide correlation

- **The remainder of "Basics" is for Domino developers, only**
  - Error string is here for reference, only. Real strings are resourced.
  - Addin name & Value is the ID of this message document
  - Old Event type is pre-D7 type, and still supported via Notes C API
  - Event type & subtype are new in D7
  - The Correlation setting defines how to locate similar reports that have been generated on other servers

Knowledge Defined in Message Documents

- **Probable Cause & Possible Solution text is also defined in the message documents**
- **Customers are free to add to this text as they see fit.**
  - We currently have about 10% of the ~6900 message document populated with Probable Cause & Possible Solution text

- **User Comments will show up in the event reports, if populated in the message document.**
  - All User Comments are shipped blank

Knowledge Defined in Message Documents

- **Corrective Actions are also defined in the message documents**

- **Actions can be written as a formula or in Lotus Script (but not both)**

- **Any event report note item referenced from the formula or LS will be replaced with the contents of that note item.**

- **We currently have about 1% of the ~6900 message document populated with corrective actions**

  – Users are encouraged to create their own corrective actions

Corrective Actions

- ## Types of Corrective Actions shipping with D7.0
  - Security Change (e.g. ECL or ACL dialog box)
  - Configuration Change (e.g. modify values of notes.ini, directory, etc.)
  - Application Change (e.g. add/remove db, enable/disable agent)
  - Initiate (e.g. agent, task, compact, fixup)
  - Terminate (e.g. agent, task)
  - Restart (e.g. task, process)
  - Reset data (e.g. clear replication history)
  - Notification (e.g. compose an e-mail)
  - Navigation to something that could be examined
    (e.g. Lotus Script profiling, a database view, etc.)

Correction, the bottom line ...

- **Knowledge pertaining to error conditions is stored in events4.nsf message documents**

- **This knowledge is displayed in an event report as probable cause text, possible solution text and clickable corrective actions**

- **Customers are encouraged to extend this knowledge base by editing events4.nsf message documents**

Beyond the Five C's of DDM

- **DDM Filters**

DDM Filters

- **7.0 event filters control what and how much information is reported to ddm.nsf. Why?**
  - Initial flood of events is striking, many of which have always been there
  - Over time, administrators will want to "adjust the volume", seeing more or less of certain events
- **Enhanced and simple events can be filtered.**
- **Filters can target specific servers and filter out events by event type/area and severity**
- **A default filter is supplied and enabled for simple events to reduce the initial "noise".**

DDM Filters

- **Defined in events4.nsf**

- **Can target specific servers**

- **Can filter both enhanced and simple events, or just simple events**

- **Can filter all event types by severity**

- **Can filter specific event types by severity**

Domino Domain Monitor Filter

Description:

hpeebles7 simple code & db

Event Filter:

○ Apply filter to enhanced and simple events
◉ Only apply filter to simple events

Event Types and Severities to Log:

○ Log All Event Types   ◉ Log Selected Event Types

		Fatal	Failure	Warning (high)	Warning (low)	Normal
☑ Application Code	☑ All Severities	☑ Fatal	☑ Failure	☑ Warning (high)	☑ Warning (low)	☑ Normal
☑ Database	☐ All Severities	☑ Fatal	☑ Failure	☑ Warning (high)	☐ Warning (low)	☐ Normal
☐ Directory	☐ All Severities	☐ Fatal	☐ Failure	☐ Warning (high)	☐ Warning (low)	☐ Normal

All servers in the domain

IBM.

7 Key Points to Take Home

- **DDM is aimed at TCO reduction and all administrators**
- **One-stop shopping for monitoring and problem resolution**
- **Distills and correlates a huge amount of otherwise indigestible data**
- **Highly usable interface allows systematic approach to server issues**
- **Configurability and flexibility accommodates diverse enterprises**
- **More efficient monitoring and problem resolution leads to:**
  - Server stability and uptime
  - Focus on business needs, not the mechanics of administration
- **DDM should become primary monitoring interface, but it's optional!**
- **DDM architecture facilitates future extensibility and programmability**

IBM.

Agenda

- Server monitoring and analysis

- Domino Domain Monitoring

- **Custom Monitoring and Third-Party Products**

Custom monitoring

- Event Handlers

- Shell/batch scripts to monitor ASCII Domino console log output

- C/C++ API Toolkit to access Domino database components

- Java/COM/OLE/LotusScript to access the Notes and Domino environment

IBM Tivoli Composite Application Manager(ITCAM) for Applications
Monitor your entire application environment

- ITCAM for Applications – Domino agent
  - Local or Remote monitoring of Domino Servers
    - Remote monitoring for Domino servers within the same domain
  - Performance Monitoring information on key Domino server components
    - Mail
    - Replication
    - Calendar
    - Database
    - Clusters
  - Out of box Domino performance reports

- Domino deep dive capabilities with IntelliWatch
  - Ability to visualize Intelliwatch data in TEP
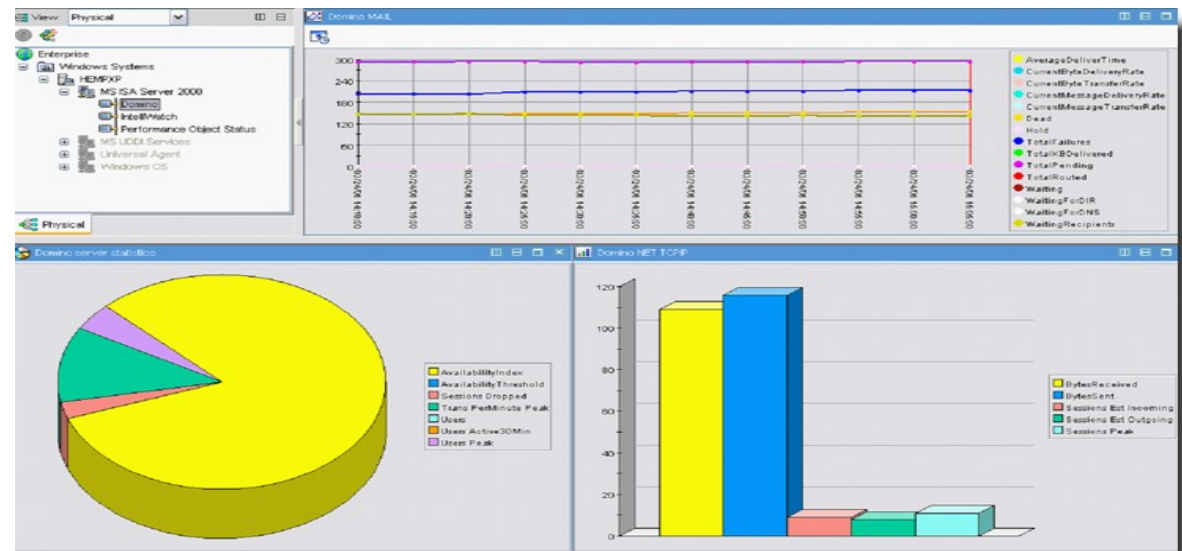
Questions?

Legal Disclaimer