

Grupo de Resposta a Incidentes de Segurança



Sistemas de Monitoramento com Alertas

Guilherme Alves Cardoso Penha
Diretor de Redes, Sites e Sistemas
guilherme@gris.dcc.ufrj.br

Grupo de Resposta a Incidentes de Segurança
Departamento de Ciência da Computação
Instituto de Matemática
Universidade Federal do Rio de Janeiro



- **Introdução**
- **Motivação**
- **O que monitorar?**
- **Qual programa faz isso? Como escolher um?**



O que é um sistema de monitoramento ?

“ É o processo contínuo e sistemático de supervisão e revisão do gerenciamento de um serviço ou uma atividade, com o objetivo de assegurar que o comportamento e o desempenho estejam de acordo com o planejado.”

Para que serve um sistema de monitoramento ?

- ♦ Analisar o comportamento do projeto
- ♦ Analisar o desempenho do projeto
- ♦ Garantir a disponibilidade do projeto
- ♦ Garantir que as atividades estão sendo executadas corretamente
- ♦ Identificar problemas de forma rápida e eficaz
- ♦ Entre outros...

Por que monitorar ?

- ♦ Manter a sua rede em pleno funcionamento
- ♦ Isolar preventivamente os problemas para evitar o tempo de inatividade
- ♦ Tomar decisões bem-informadas para maximizar os recursos essenciais
- ♦ Aumentar a satisfação e a produtividade do seu projeto
- ♦ Entre outros...

O que monitorar ?

- ◆ **Ativos da Rede**
- ◆ **Processos Críticos**
- ◆ **Recursos do Sistema**
- ◆ **Desempenho do Sistema**
- ◆ **Informações Sensíveis**
- ◆ **Entre outros...**



O que monitorar?



- **Ativos da Rede**

- **A máquina está ligada?**
- **Foi reiniciada? Quando?**



- **Processos Críticos**

- **Servidor Web**
- **Servidor de Email**
- **Servidor de Banco de Dados**
- **Repositório de Arquivos**



- **Recurso e Desempenho do Sistema**
 - **Consumo de Memória aceitável?**
 - **Consumo de CPU aceitável?**
 - **Consumo de Recurso por aplicativo?**

O que monitorar?

III
Workshop

- **Informações Sensíveis**

- **Permissão**
- **Data de Criação/Modificação (timestamp)**
- **Tamanho**
- **Checksum**



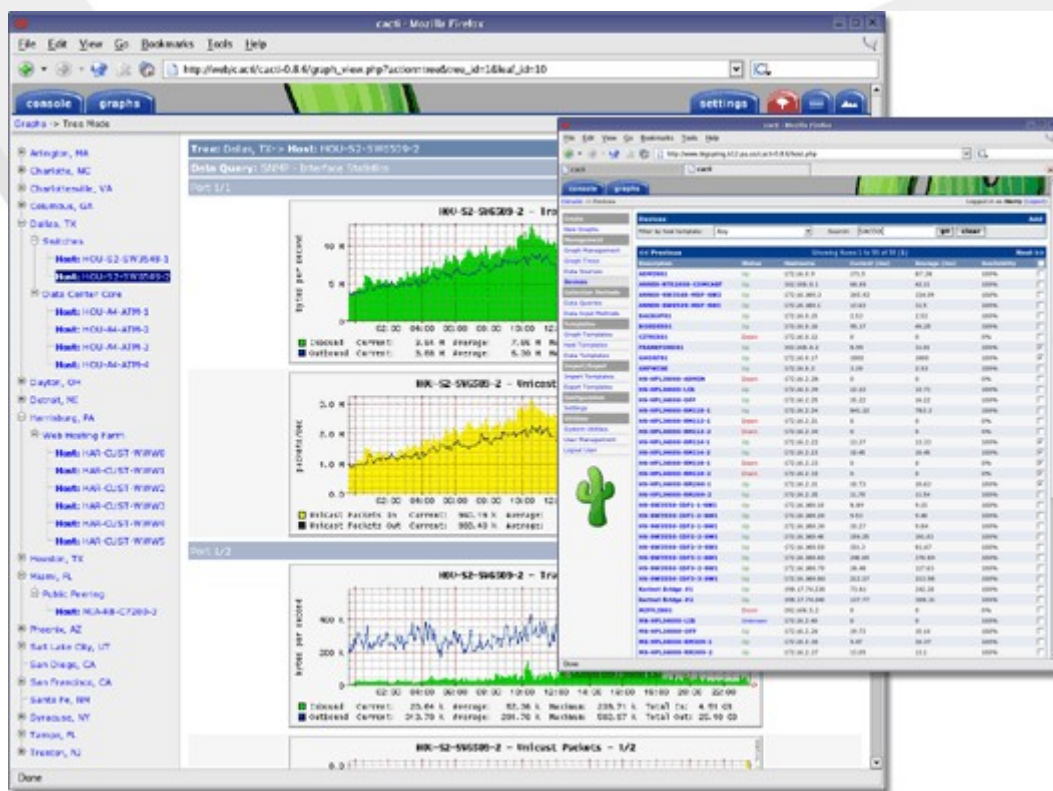
- Alterações em arquivos
- Análise de Registros (logs) do sistema
- Conexões por protocolo
- Conexões com requisições reais
- Ping

Programas Existentes

III
Workshop

CACTI

Site: <http://cacti.net>



Grupo de Resposta a Incidentes de Segurança
Departamento de Ciência da Computação
Instituto de Matemática
Universidade Federal do Rio de Janeiro

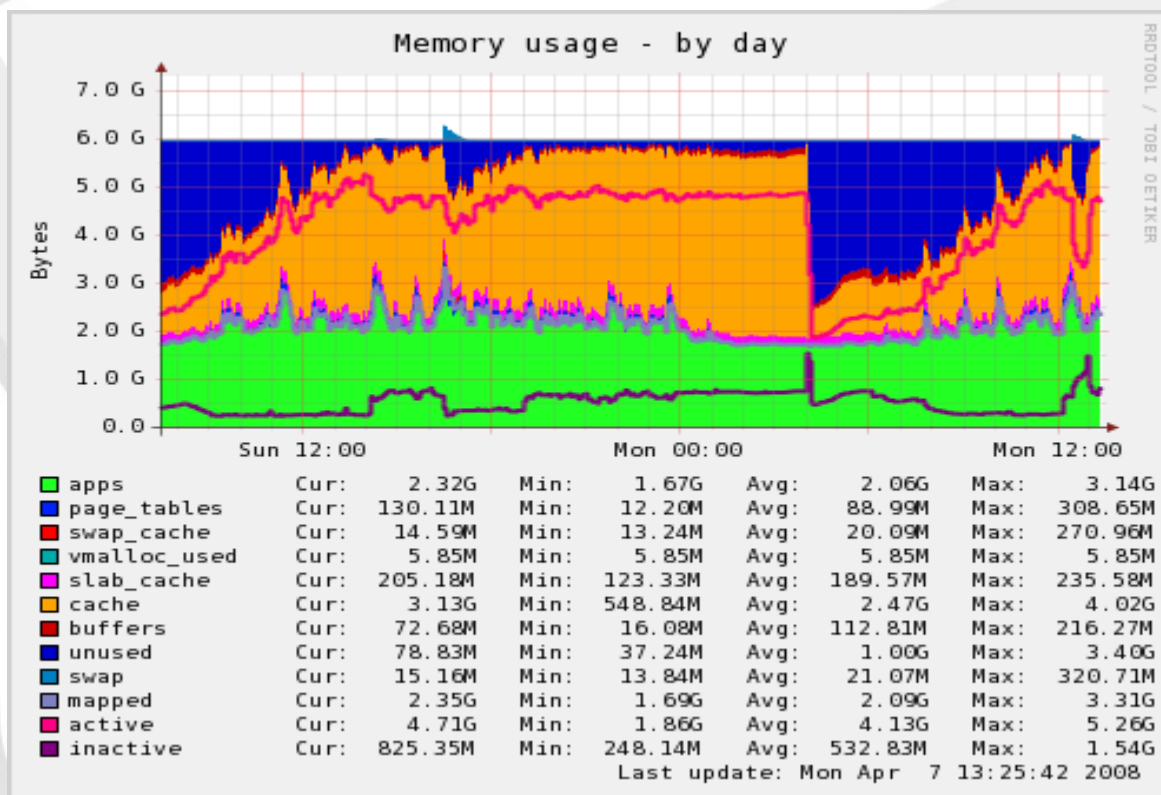
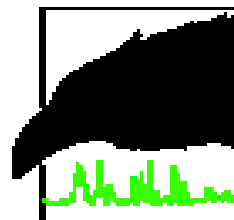


Programas Existentes

III
Workshop

MUNIN

Site: <http://munin.projects.linpro.no>



Grupo de Resposta a Incidentes de Segurança
Departamento de Ciência da Computação
Instituto de Matemática
Universidade Federal do Rio de Janeiro



Programas Existentes

III Workshop

NAGIOS

Site: <http://www.nagios.org>

N

Nagios

General

- Home
- Documentation

Monitoring

- Tactical Overview
- Service Detail
- Host Detail
- Status Overview
- Status Summary
- Status Grid
- Status Map
- 3-D Status Map
- Service Problems
- Host Problems
- Network Outages
- Comments
- Downtime
- Process Info
- Performance Info
- Scheduling Queue

Reporting

- Trends
- Availability
- Alert Histogram
- Alert History
- Alert Summary
- Notifications
- Event Log

Current Network Status
Last Updated: Wed Jan 19 14:47:28 CET 2005
Updated every 90 seconds
Nagios® - www.nagios.org
Logged in as: nagios

[View History For all hosts](#)
[View Notifications For All Hosts](#)
[View Host Status Detail For All Hosts](#)

Host Status Totals

Up	Down	Unreachable	Pending
78	1	0	0

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
79	3	0	1	0

Service Status Details For All Hosts

Host	Service	Status	Last Check	Duration	Attempt	Status Information
Lissac-Angers	PING	OK	19-01-2005 14:45:51	0d 0h 1m 28s	1/3	PING OK - Packet loss = 0%, RTA = 61.14 ms
Lissac-Angers-Neuf	PING	OK	19-01-2005 14:45:10	0d 0h 2m 8s	1/3	PING OK - Packet loss = 0%, RTA = 76.30 ms
Lissac-Angers-Wanadoo	PING	OK	19-01-2005 14:45:59	0d 0h 1m 18s	1/3	PING OK - Packet loss = 0%, RTA = 63.72 ms
Lissac-Argenteuil	PING	OK	19-01-2005 14:45:10	0d 0h 2m 8s	1/3	PING OK - Packet loss = 0%, RTA = 67.86 ms
Lissac-Argenteuil-Neuf	PING	OK	19-01-2005 14:43:45	0d 8h 40m 18s	1/3	PING OK - Packet loss = 0%, RTA = 85.81 ms
Lissac-Argenteuil-Wanadoo	PING	OK	19-01-2005 14:43:46	0d 20h 20m 18s	1/3	PING OK - Packet loss = 0%, RTA = 80.56 ms
Lissac-Auber	PING	OK	19-01-2005 14:44:43	0d 0h 2m 38s	1/3	PING OK - Packet loss = 0%, RTA = 127.01 ms
Lissac-Bordeaux	PING	OK	19-01-2005 14:43:02	0d 2h 49m 18s	1/3	PING OK - Packet loss = 0%, RTA = 107.64 ms
Lissac-Boulogne	PING	OK	19-01-2005 14:45:42	0d 4h 56m 38s	1/3	PING OK - Packet loss = 0%, RTA = 76.50 ms



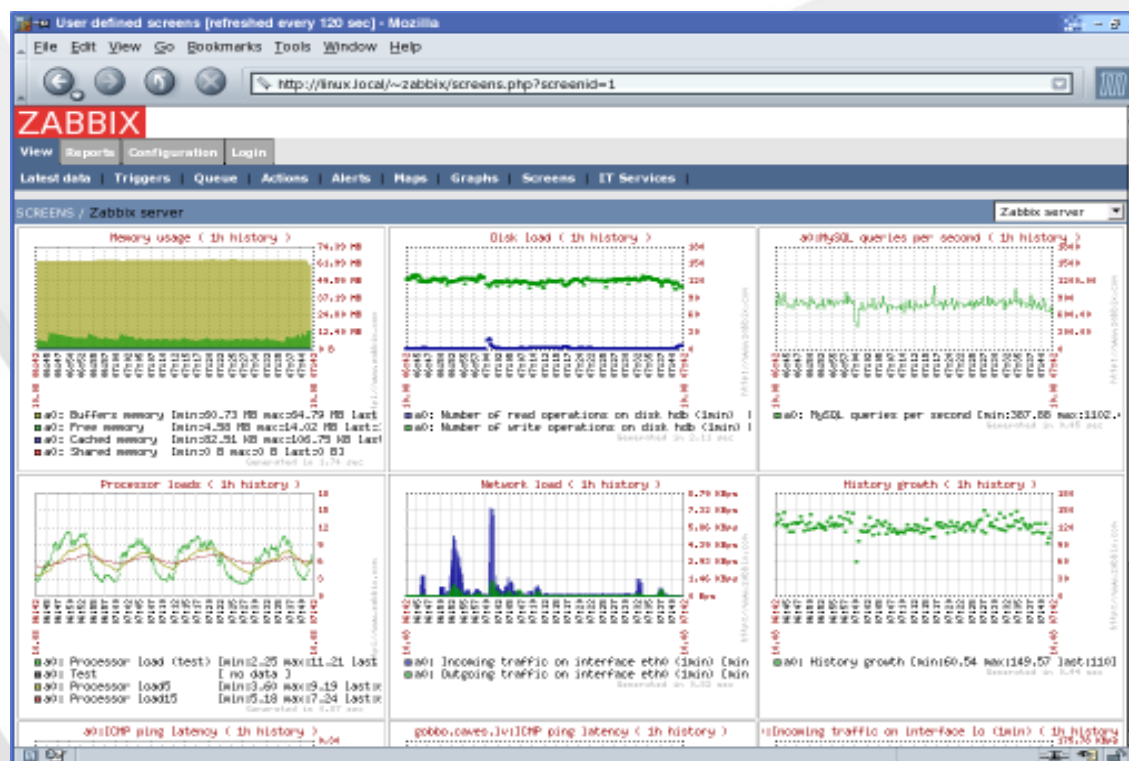
Programas Existentes

III
Workshop

ZABBIX

Site: <http://www.zabbix.com>

ZABBIX



Grupo de Resposta a Incidentes de Segurança
Departamento de Ciência da Computação
Instituto de Matemática
Universidade Federal do Rio de Janeiro



Programas Existentes

III
Workshop

ZENOSS

Site: <http://www.zenoss.com>

Zenoss®

The screenshot shows the Zenoss Enterprise web interface. The top navigation bar includes a 'Device/IP Search' field, links for 'admin', 'Preferences', 'Logout', and 'Help', and the 'Zenoss server time: 12:40:01'. The left sidebar contains a 'Main Views' section with links to 'Dashboard', 'Event Console', 'Device List', and 'Network Map'. Below this is a 'Classes' section with links to 'Events', 'Devices', 'Services', 'Processes', and 'Products'. The 'Browse By' section includes links to 'Systems', 'Groups', 'Locations', 'Networks', and 'Reports'. The 'Management' section includes links to 'Add Device', 'Mibs', 'Collectors', 'Settings', and 'Event Manager'. The main content area is divided into three panels. The 'Locations' panel on the left shows a map of North America with callouts for 'Click to toggle menu visibility' and 'Navigation Menu: Navigate Zenoss views and select tasks'. The 'Root Organizers' panel on the right has a callout 'Manage and configure the dashboard' and contains two tables. The top table lists system objects and their event counts, while the bottom table lists group objects and their event counts. A callout 'Configure this portlet' points to the bottom table.

Object	Events
/Systems/Development	1
/Systems/Testing	1
/Systems/Trading	1
/Systems/BlahBlahBlah	1
/Systems/Network	1
/Systems/Buildbot	
/Systems/CRM	
/Systems/Internet	

Object	Events
/Groups/Admin 1 Group	1
/Groups/Support	1
/Groups/build	1
/Groups/Network	
/Groups/Customers	

Grupo de Resposta a Incidentes de Segurança
Departamento de Ciência da Computação
Instituto de Matemática
Universidade Federal do Rio de Janeiro

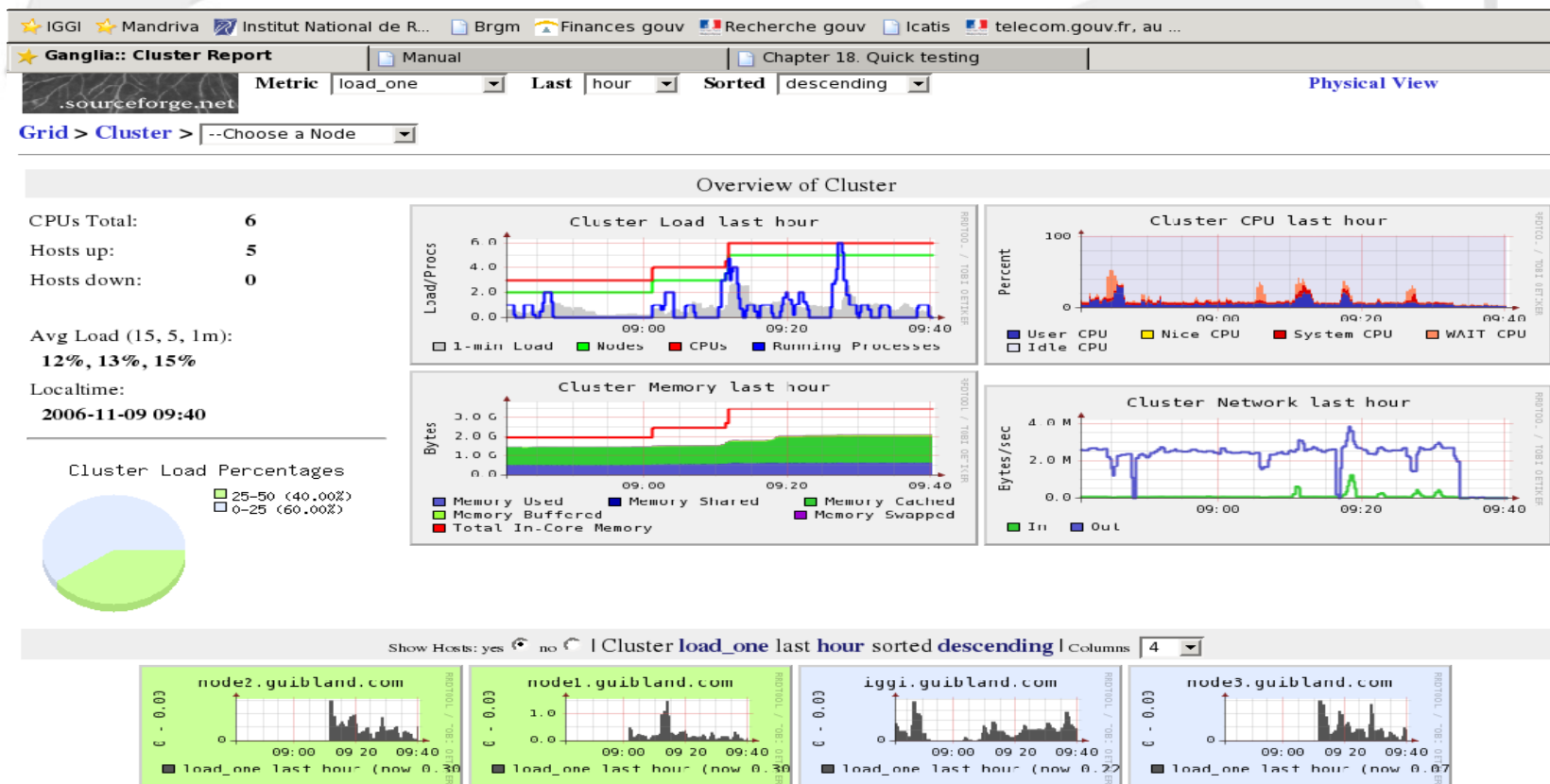


Programas Existentes

III
Workshop

GANGLIA

Site: <http://ganglia.info>



Grupo de Resposta a Incidentes de Segurança
Departamento de Ciência da Computação
Instituto de Matemática
Universidade Federal do Rio de Janeiro

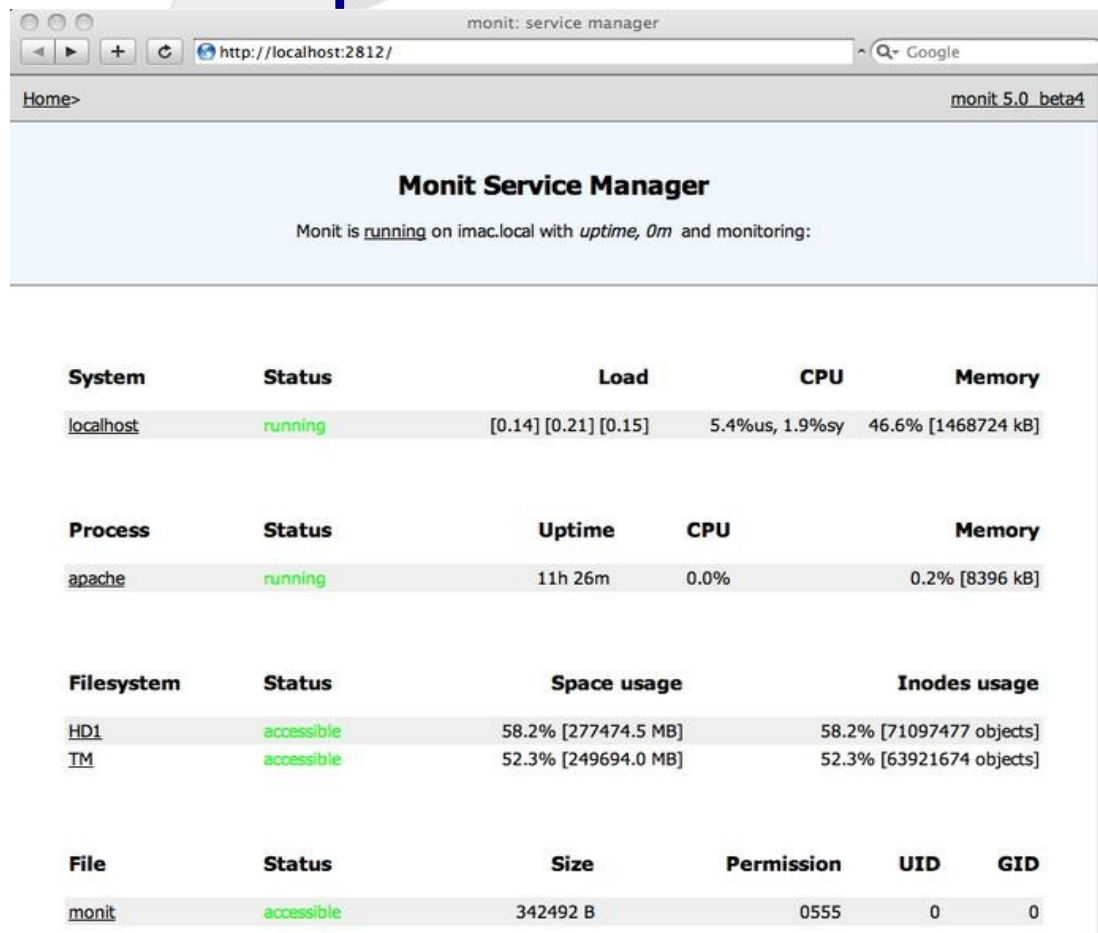


Programas Existentes

III
Workshop

MONIT

Site: <http://mmonit.com/monit>



System	Status	Load	CPU	Memory
localhost	running	[0.14] [0.21] [0.15]	5.4%us, 1.9%sy	46.6% [1468724 kB]

Process	Status	Uptime	CPU	Memory
apache	running	11h 26m	0.0%	0.2% [8396 kB]

Filesystem	Status	Space usage	Inodes usage
HD1	accessible	58.2% [277474.5 MB]	58.2% [71097477 objects]
TM	accessible	52.3% [249694.0 MB]	52.3% [63921674 objects]

File	Status	Size	Permission	UID	GID
monit	accessible	342492 B	0555	0	0



Grupo de Resposta a Incidentes de Segurança
Departamento de Ciência da Computação
Instituto de Matemática
Universidade Federal do Rio de Janeiro



Como escolher um programa?

- **Atenda suas necessidades específicas**
- **Possua criptografia na conexão com o cliente**
- **Seja fácil de utilizar**
- **Seja de fácil configuração e manutenção**



Restringindo o acesso

- **Proteja com htaccess:**
 - **Arquivos de Configuração**
 - **Interface administrativa**
 - **Relatórios**

O que o Monit tem de vantagem?

- Alerta em tempo real por email
SMS para operadoras compatíveis
- Controle e acesso pelo Console e Navegador
Praticidade



O que o Monit tem de vantagem?

- Geração de log's pelo Syslog e direto no arquivo
Compatibilidade
- Resposta imediata
Realiza tarefa programada para cada caso

O que o Monit tem de vantagem?

- Tamanho reduzido
Aproximadamente 300kb
- Servidor HTTP(S) próprio
Independente do servidor web da máquina

O que o Monit tem de vantagem?

- Integração com o M/Monit
Monitoramento e manutenção distribuída
- Suporte eficiente
Desenvolvedores e Comunidade

Grupo de Resposta a Incidentes de Segurança



Documentos de apoio:

- Tutorial Monit – Aplicativo para Administração Segura - <http://www.gris.dcc.ufrj.br>
<http://www.gris.dcc.ufrj.br/bd/tutoriais/GRIS-2009-T-001.pdf>
- Site oficial de cada ferramenta

