PEN

PROCESSO ELETRÔNICO NACIONAL

Processo Eletrônico Nacional

SECRETARIA DE GESTÃO

MINISTÉRIO DO PLANEJAMENTO, DESENVOLVIMENTO E GESTÃO

BRASIL GOVERNO FEDERAL

Tópicos apresentação

- Componentes de software da solução
- Mecanismos de autenticação e autorização
- Infraestrutura hardware sugerida para o SEI
- Avaliação da infraestrutura para atendimento à carga de usuários
- Gargalos eventuais em banco de dados já observados
- Portabilidade para outros SGDBs (viabilidade / esforço necessário);
- Mecanismos de segurança
- Processo de assinatura e verificação de assinatura digital
- Mecanismo de armazenamento dos documentos e metadados
- Política e infraestrutura de backup

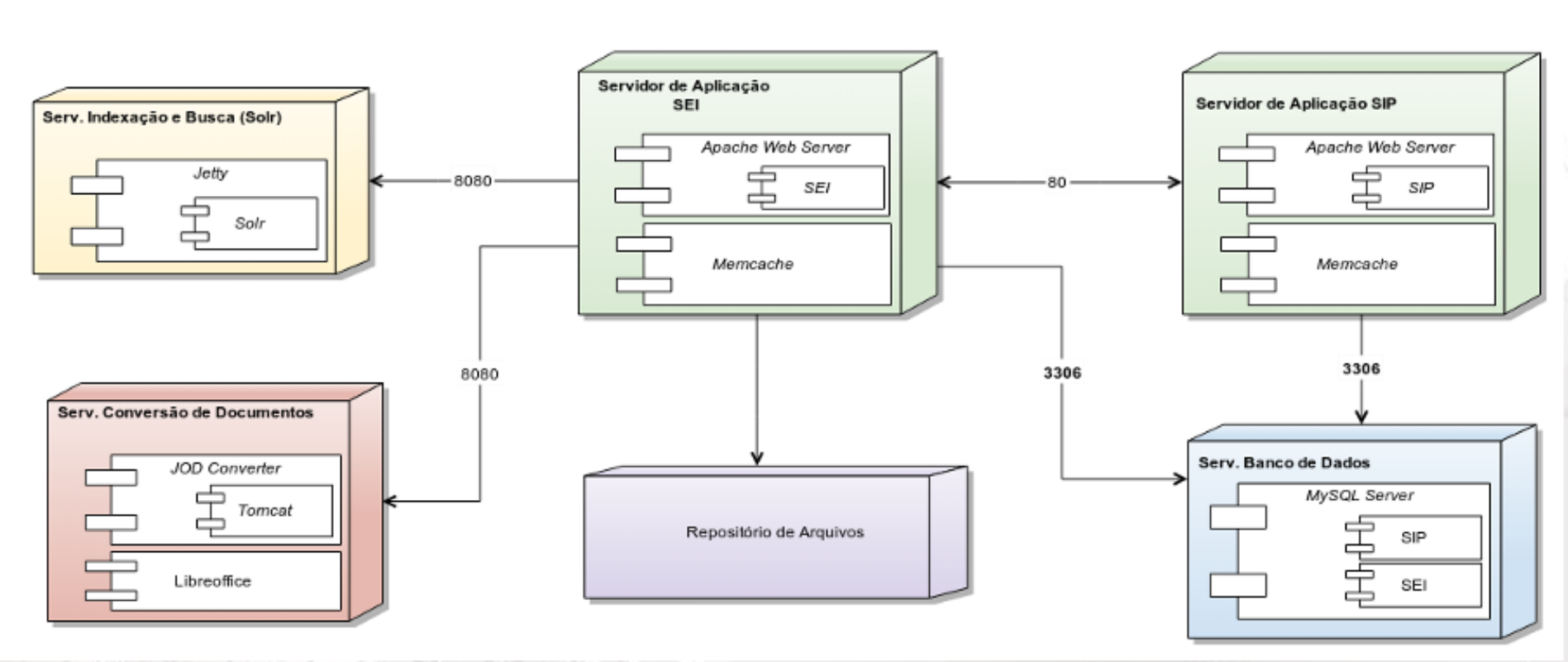
Alguns Números do SEI (MP)

- Usuários atendidos: **5.160**
- **62,00** requisições por segundo
- **94,00** Gb transferidos/dia
- **2.000.000** acessos/dia
- Unidades Administrativas: **714 (em 66 cidades)**
- Processos: **556.684**
- Documentos: **1035.800 (49% gerados)**
- Base de Dados: **206 Gb**
- Repositório de Arquivos: **3,3 TBs**

Alguns Números do SEI (TRF4)

	2012	2013	2014	2015	2016
Usuários	3.569	4.045	4.634	4.796	5.170
Processos	87.918	125.719	168.388	182.833	228.110
Documentos Gerados	479.930	715.830	994.273	1.100.061	1.451.472
Tamanho da Base (Gb)	15	55	98	117	159
Documento Externos	493.796	715.830	1.032.705	1.141.716	1.498.641
Tamanho do Repositório (Gb)	365	623	871	964	1.410

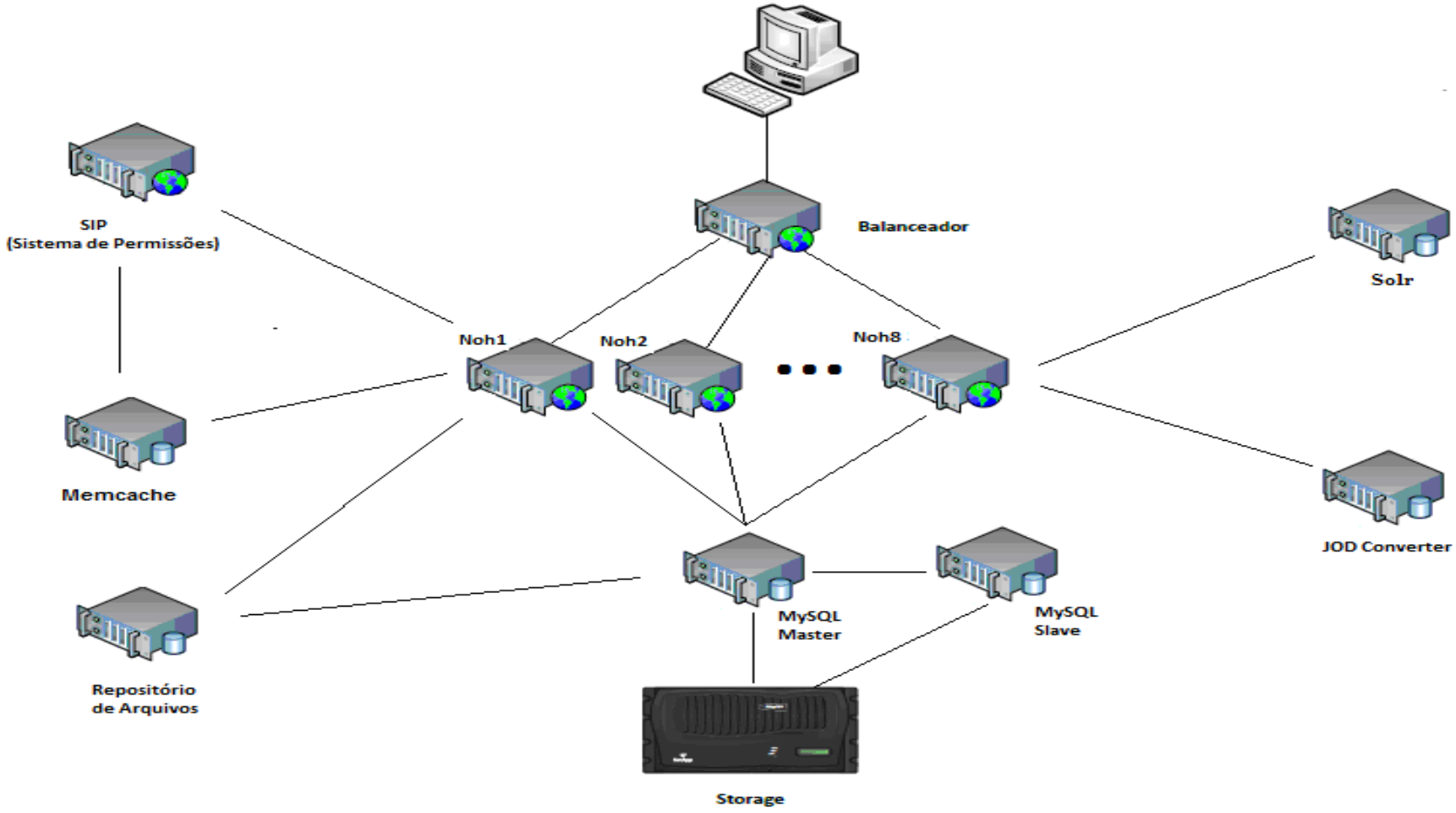
Componentes do Sistema



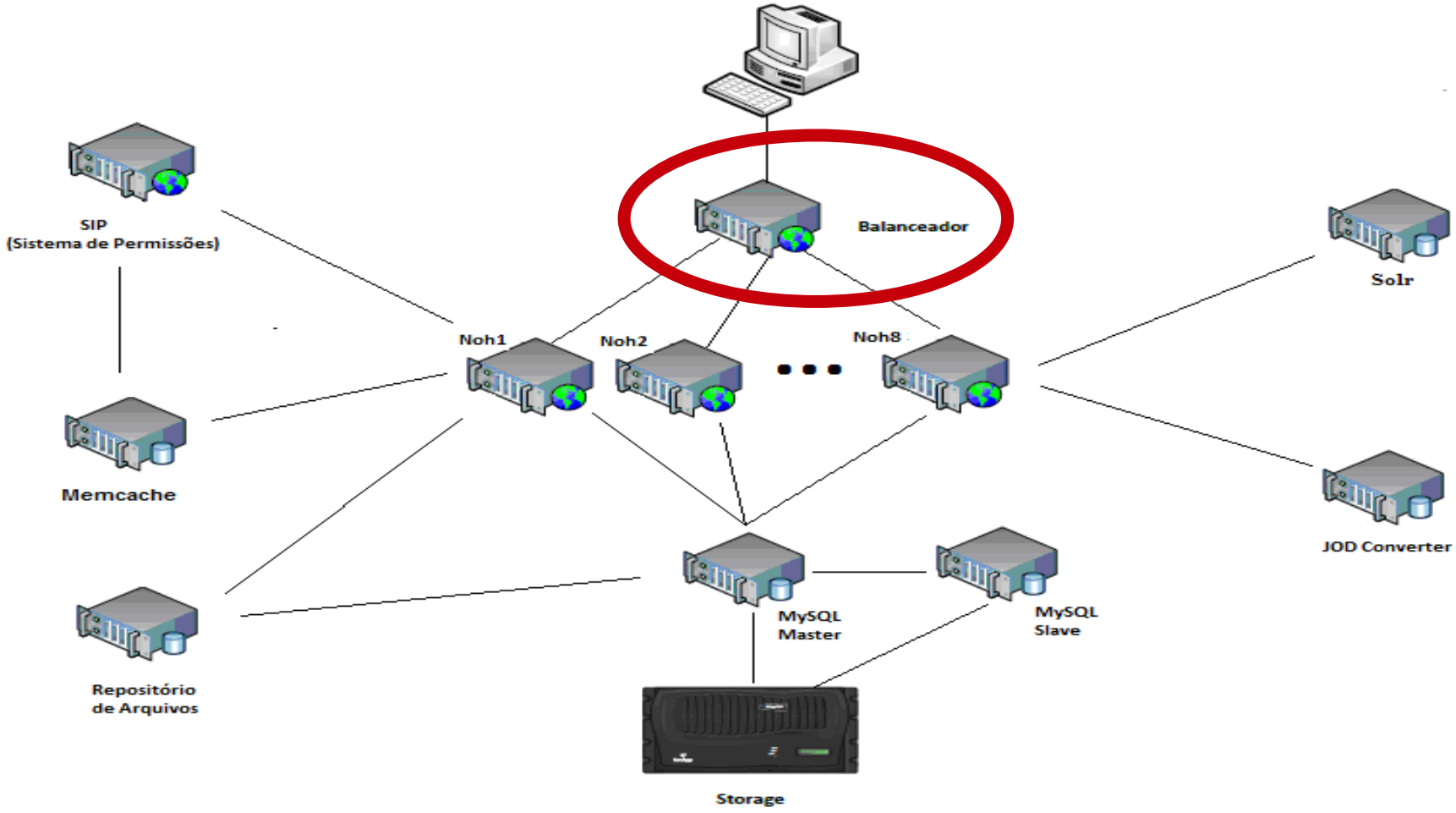
Componentes do Sistema – Cont.

SEI	3.0.1
SIP	3.0.1
MySQL Server	5.6.X
Apache Web Server	2.4.6
Memcache	3.0.8
PHP 5	5.6.5
Apache Solr	6.1.X
JOD Converter	2.2.2

Infraestrutura de Hardware Sugerida



Infraestrutura de Hardware Sugerida

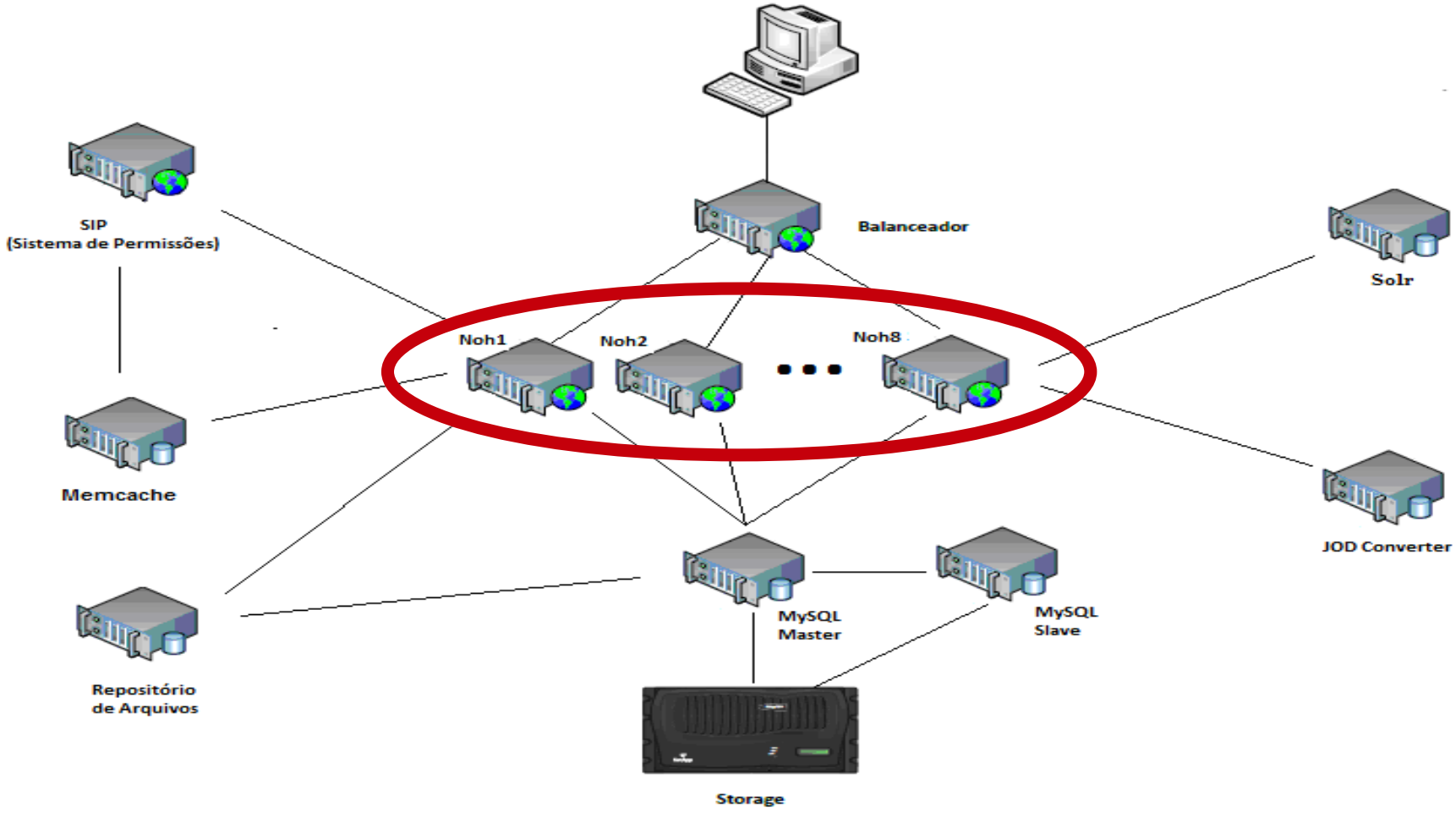


Infraestrutura de Hardware Sugerida

- Balanceador de Aplicação

- Componentes de software da solução
- Sistema Operacional: **Red Hat Enterprise Linux 7.1**
- Memória: **2 GB**
- Disco: **13 GB**
- CPUs: **1**
- Serviços:
  - **Apache 2.4.6**
  - **mod_proxy_balancer**
  - **mod_evasive *****

Infraestrutura de Hardware Sugerida



Infraestrutura de Hardware Sugerida

Nós de Aplicação (8)

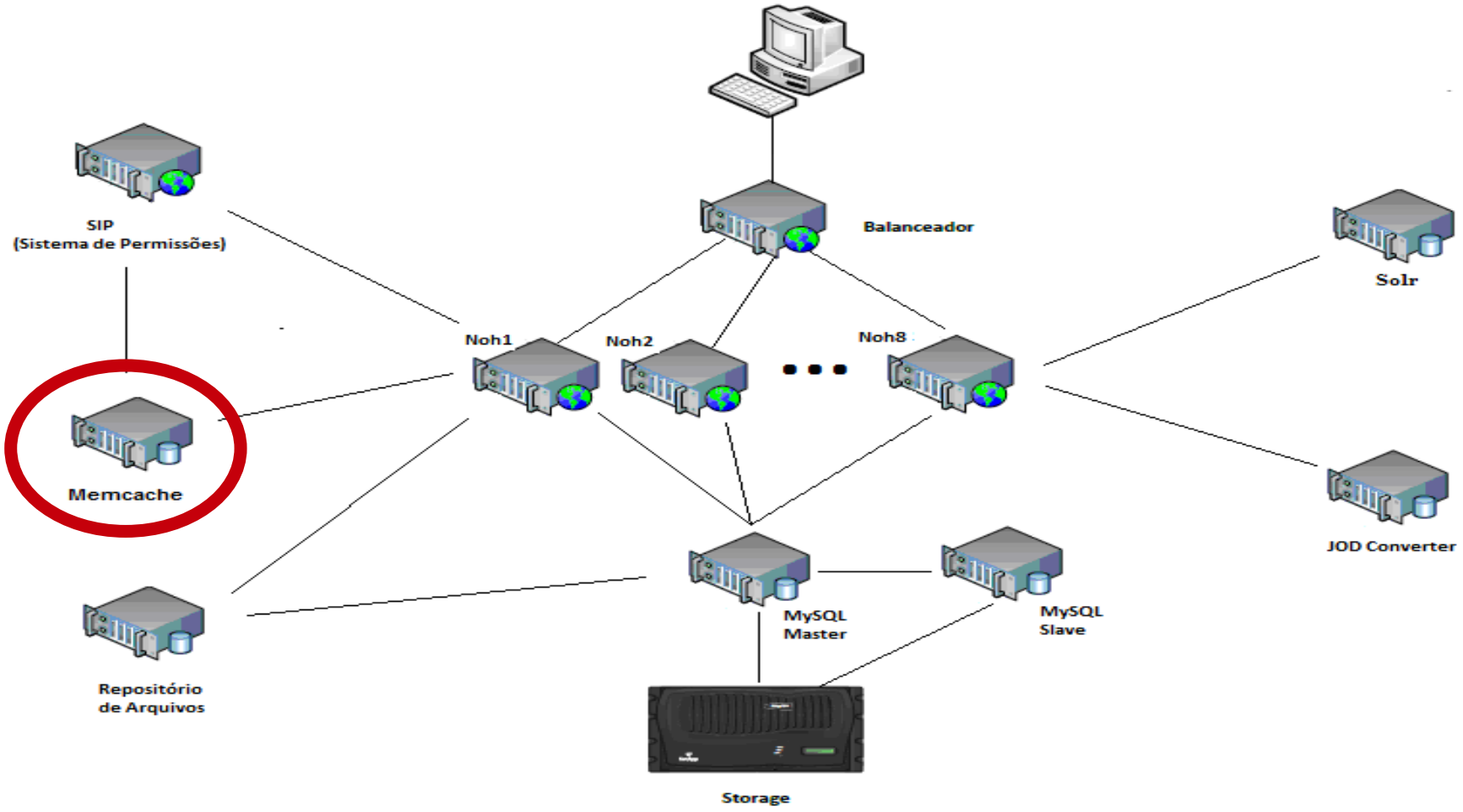
- Máquina Virtual (VMWare)
- Sistema Operacional: **Red Hat Enterprise Linux 7.1**
- Memória: **8 GB**
- Disco: **50 GB**
- CPUs: **2**
- Serviços:
  - **Apache 2.4.6**
  - **PHP 5.6.5**
  - **Aplicação SEI**
  - **MySQLi 5 ● MSSQL/FreeTDS 0.95 ● OCI8 2.0.5**
  - **Fontes True Type**

Experiência TRF4

Nós de Aplicação

- Máquina física anterior: 2 Quad-Core Intel Xeon, 2667
- MHz, 32Gb (até Setembro/2012)
- Experiência 1: 4 VMs com 1 processador e 16 Gb
- Experiência 2: 4 VMs com 2 processadores e 16 Gb
- **Experiência 3: 8 VMs com 1 processador e 8 Gb**
- Experiência 4: 12 VMs com 1 processador e 8 Gb

Infraestrutura de Hardware Sugerida

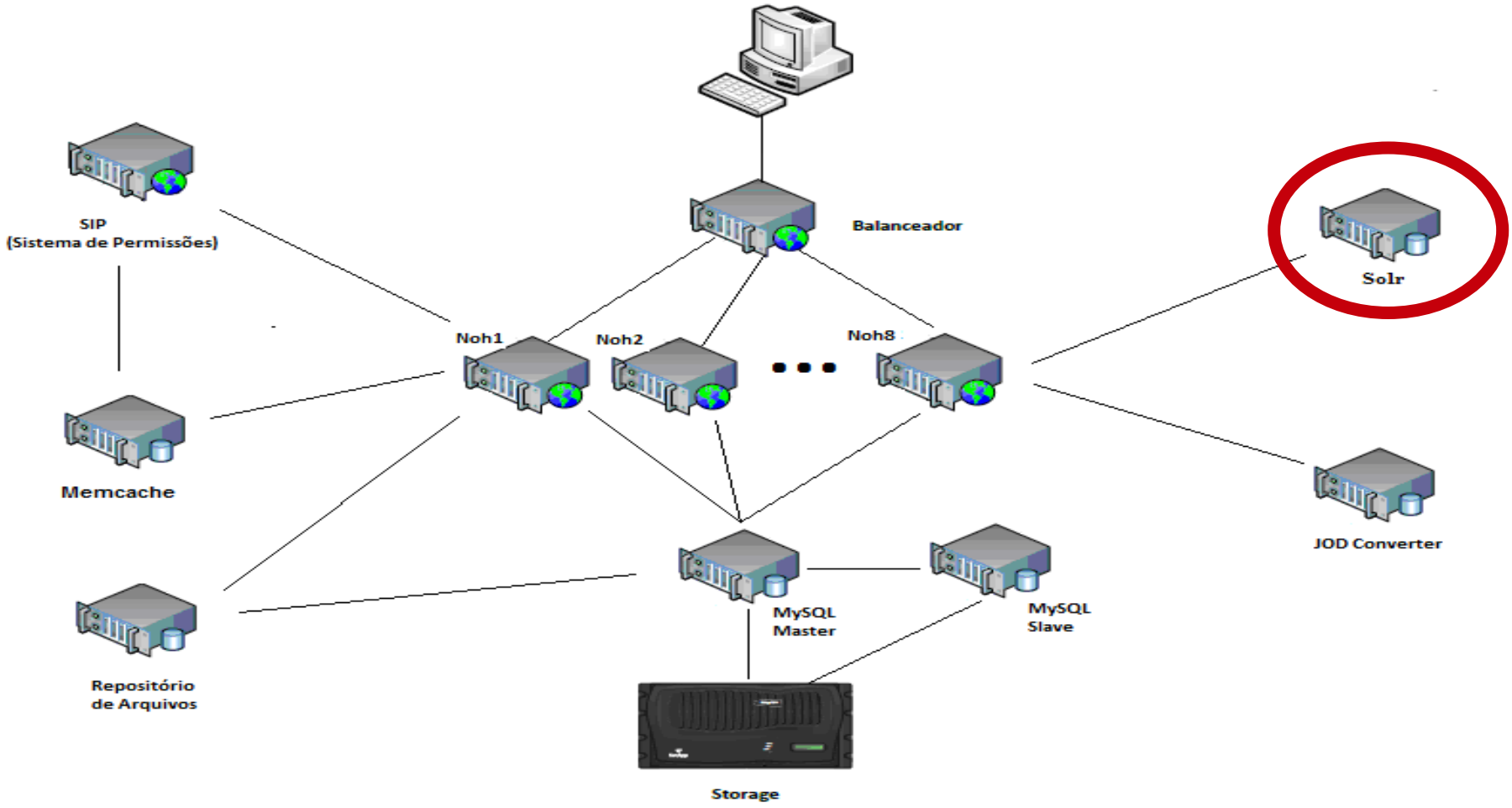


Infraestrutura de Hardware Sugerida

Serviço de Cache (Memcache)

- Máquina Virtual (VMWare)
- Sistema Operacional: **Red Hat Enterprise Linux 7.1**
- Memória: **4 GB**
- Disco: **24 GB**
- CPUs: **1**
- Serviços:
  - **Apache 2.4.6**
  - **Memcache 3.0.8 (serviço memcached)**

Infraestrutura de Hardware Sugerida



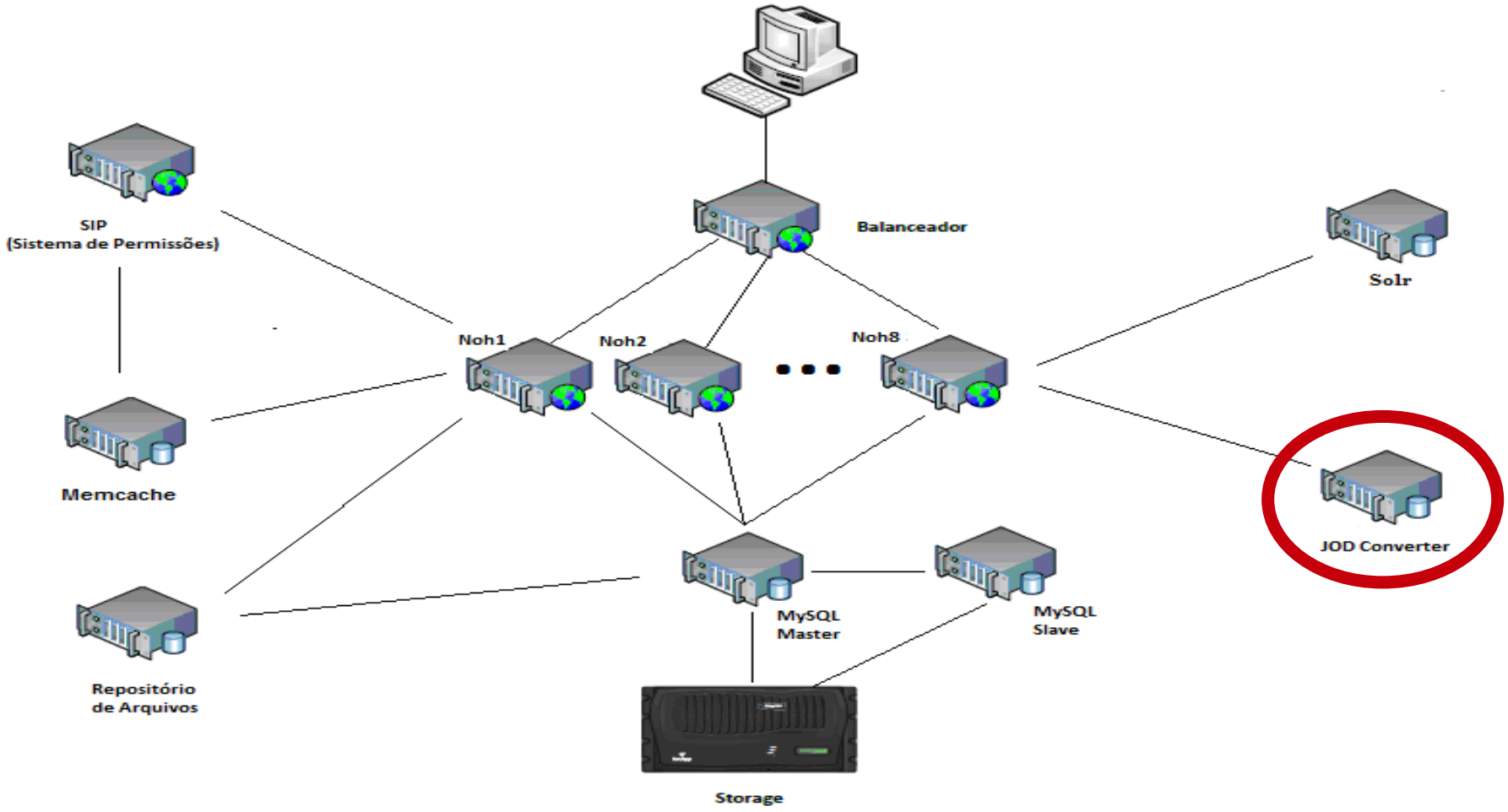
Infraestrutura de Hardware Sugerida

Mecanismo de Busca (Apache Solr)

- Máquina Virtual (VMWare)
- Sistema Operacional: **Red Hat Enterprise Linux 7.1**
- Memória: **8 GB**
- Disco: **50 Gb** (diretório /tmp com no mínimo 2Gb livres)
- CPUs: **2**
- Serviços:
  - **Solr 6.1.0**
  - **Java runtime 1.8**

- *** Entre 1.200 e 1500 pesquisas diárias*

Infraestrutura de hardware proposta

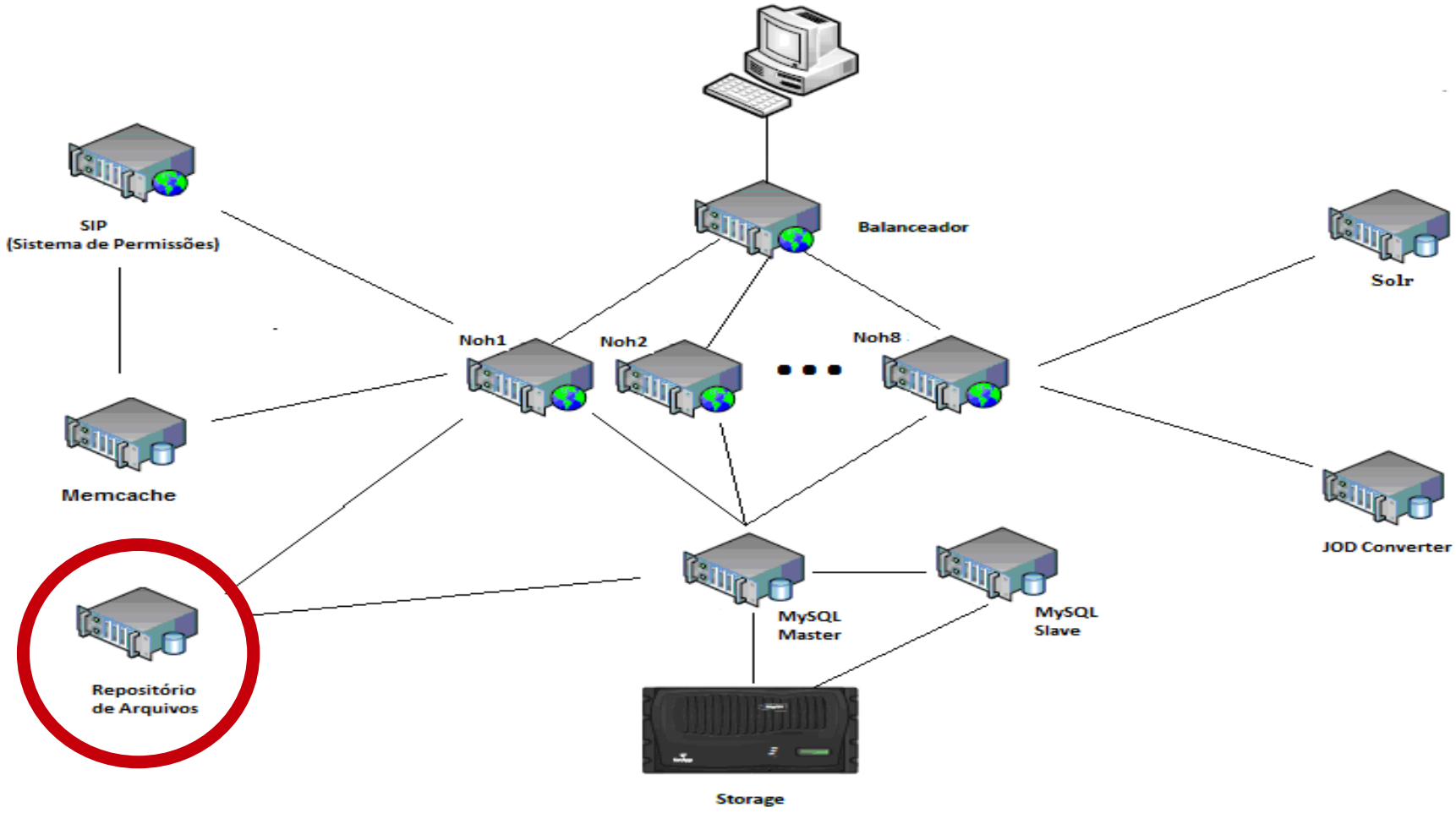


Infraestrutura de Hardware Sugerida

Geração de PDFs (JOD Converter)

- Máquina Virtual (VMWare)
- Sistema Operacional: **Red Hat Enterprise Linux 7.1**
- Memória: **8 GB**
- Disco: **50 GB**
- CPUs: **1**
- Serviços:
  - **Java runtime 1.7**
  - **LibreOffice**
  - **Tomcat 6**

Infraestrutura de Hardware Sugerida



Infraestrutura de Hardware Sugerida

Repositório de Arquivos

- Máquina física
- Sistema Operacional: **Red Hat Enterprise Linux 7.1**
- Memória: **48 GB**
- Disco: **1.2 Teras**
- CPUs: **2 Quad-Core Intel Xeon, 2667 MHz**
- Serviços:
  - **NFS**

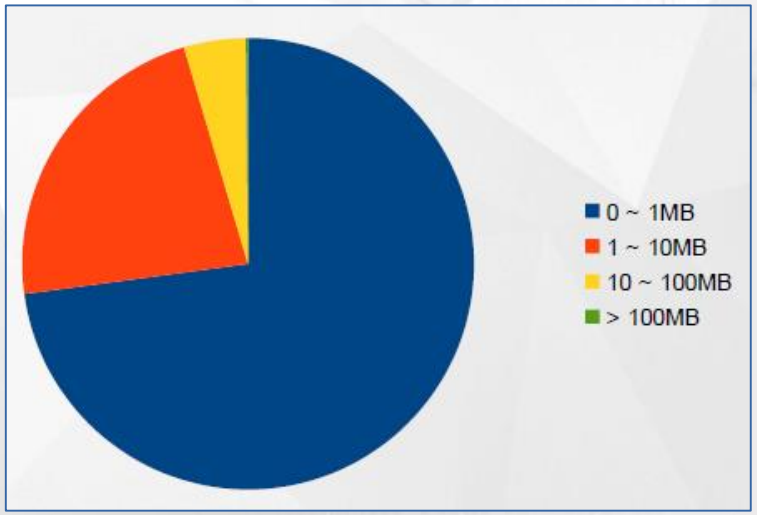
Documentos externos são armazenados em uma estrutura de diretórios associados com um hash na base de dados.

Tipos de Arquivos

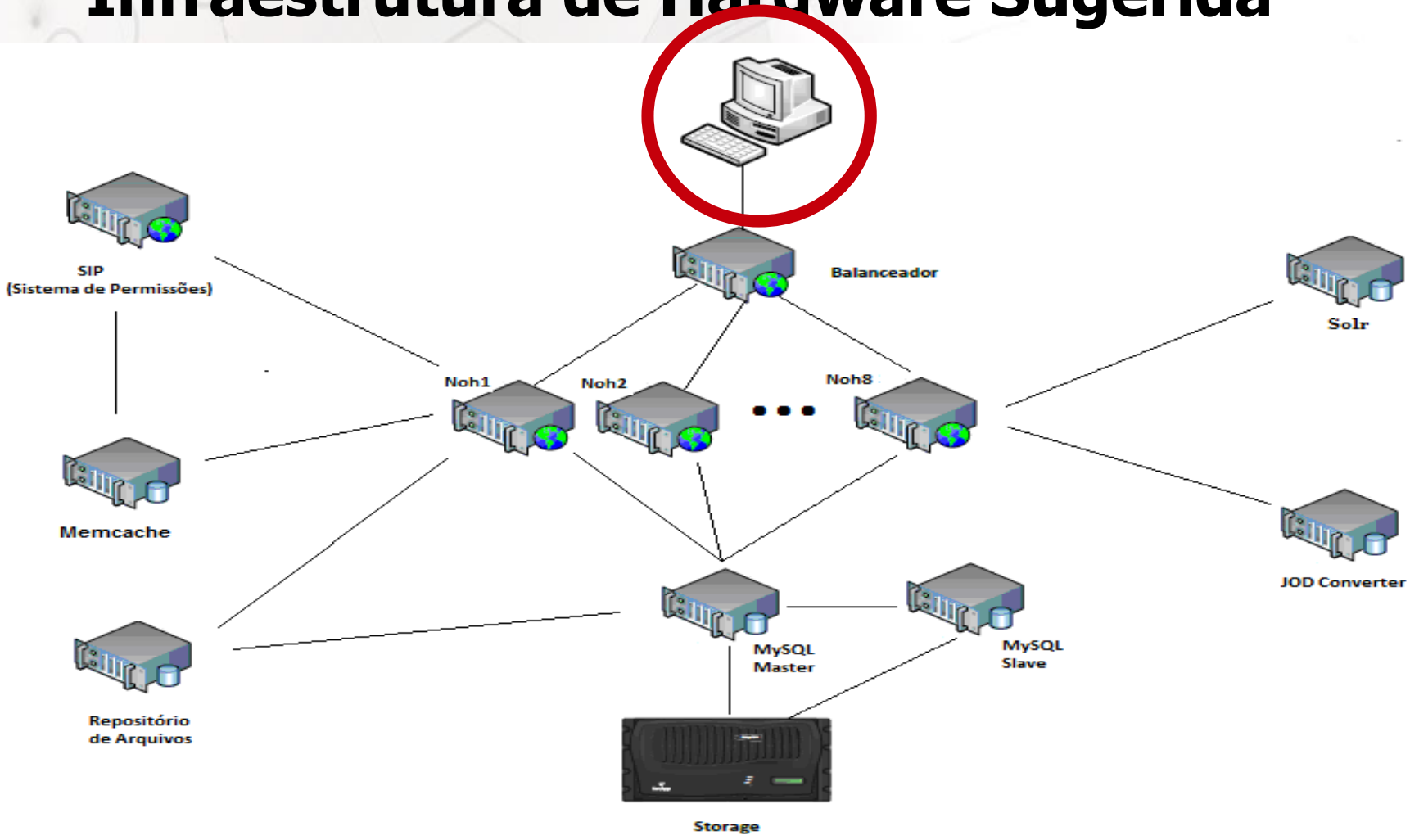
DOCUMENTOS E PUBLICAÇÕES	
html	HTML (.html ou .htm), conforme especificações do W3C
txt	Texto puro (arquivo .txt)
odg/odp/ods/odt	Open Document ODF 1.2 – especificação OASIS
pdf	Portable Document Format – PDF ISO 32000-1:2008 e PDF/A NBR ISO 19005-1:2009
GRÁFICOS E IMAGENS ESTÁTICAS	
png	W3C PNG (.png), ISO/IEC 15948:2003 (E)
svg	SVG (.svg), gerado conforme especificações do W3C
jpeg/jpg	JPEG File Interchange Format (.jpeg, .jpg ou .jfif)
ÁUDIO	
ogg /oga	Ogg Vorbis e Ogg FLAC
flac	FLAC (.flac)
VÍDEO	
ogg / ogv	Ogg Theora
mp4	Áudio e vídeo MPEG-4, Part 14
COMPACTAÇÃO DE ARQUIVOS	
zip	ZIP
gz	GNU ZIP

Repositório de Arquivos (Tipos permitidos)

- Quantidade de arquivos: 1.487.670
- Tamanho médio: 2,20 MB
  - 0~1 Mb: 72,87% (1.084.071)
  - 1~10 Mb : 22,56% (335.553)
  - 10~100 Mb: 4,42% (65.683)
  - > 100Mb: 0,16% (2.363)
- **Tipos de arquivo mais utilizados**
  - PDF: **90,58%** (1.470.510)
  - HTML: **4,16%** (67.508)
  - JPG: **1,47%** (27.994)
  - DOC: **0,91%** (14.846)



Infraestrutura de Hardware Sugerida



Infraestrutura de Hardware Sugerida

Estação-Cliente

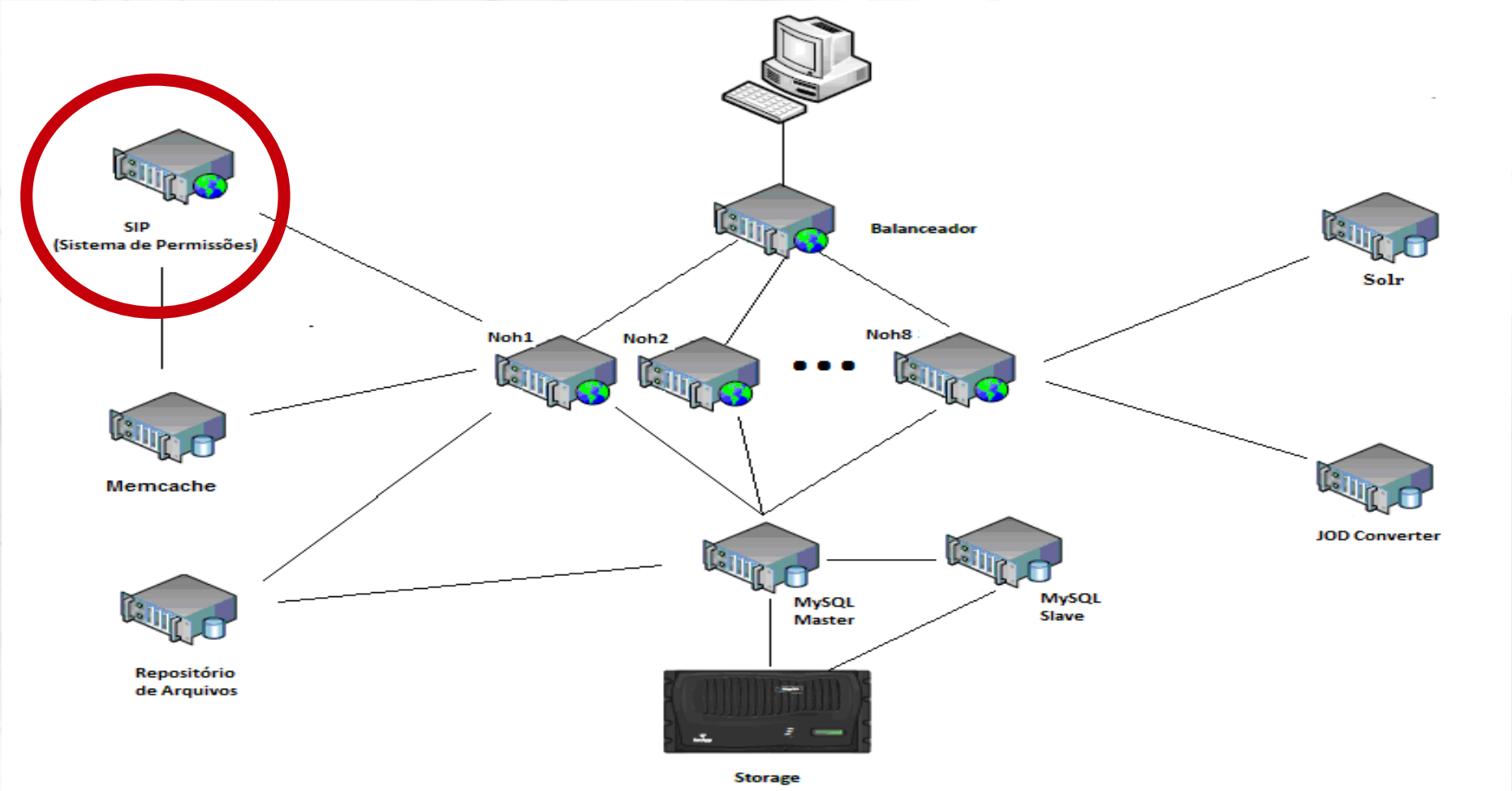
- Browsers suportados:
  - Internet Explorer 9+
  - Chrome 8+
  - Firefox 10+ ou Safari 3+;
- Recomendação Firefox/Chrome atualizados
- Configurar o desbloqueio de pop-ups
- Java Runtime 1.7 ou superior (se utilizando assinatura digital)

Infraestrutura de Hardware Sugerida

Assinatura Digital

- Java Runtime 1.7 ou superior
- Certificado compatível com o navegador
- Certificados novos “Cadeia V2” (chave 2048 bits) requerem no mínimo Windows XP com SP3

Infraestrutura de hardware proposta



Infraestrutura de Hardware Sugerida

SIP (Sistema de Permissões)

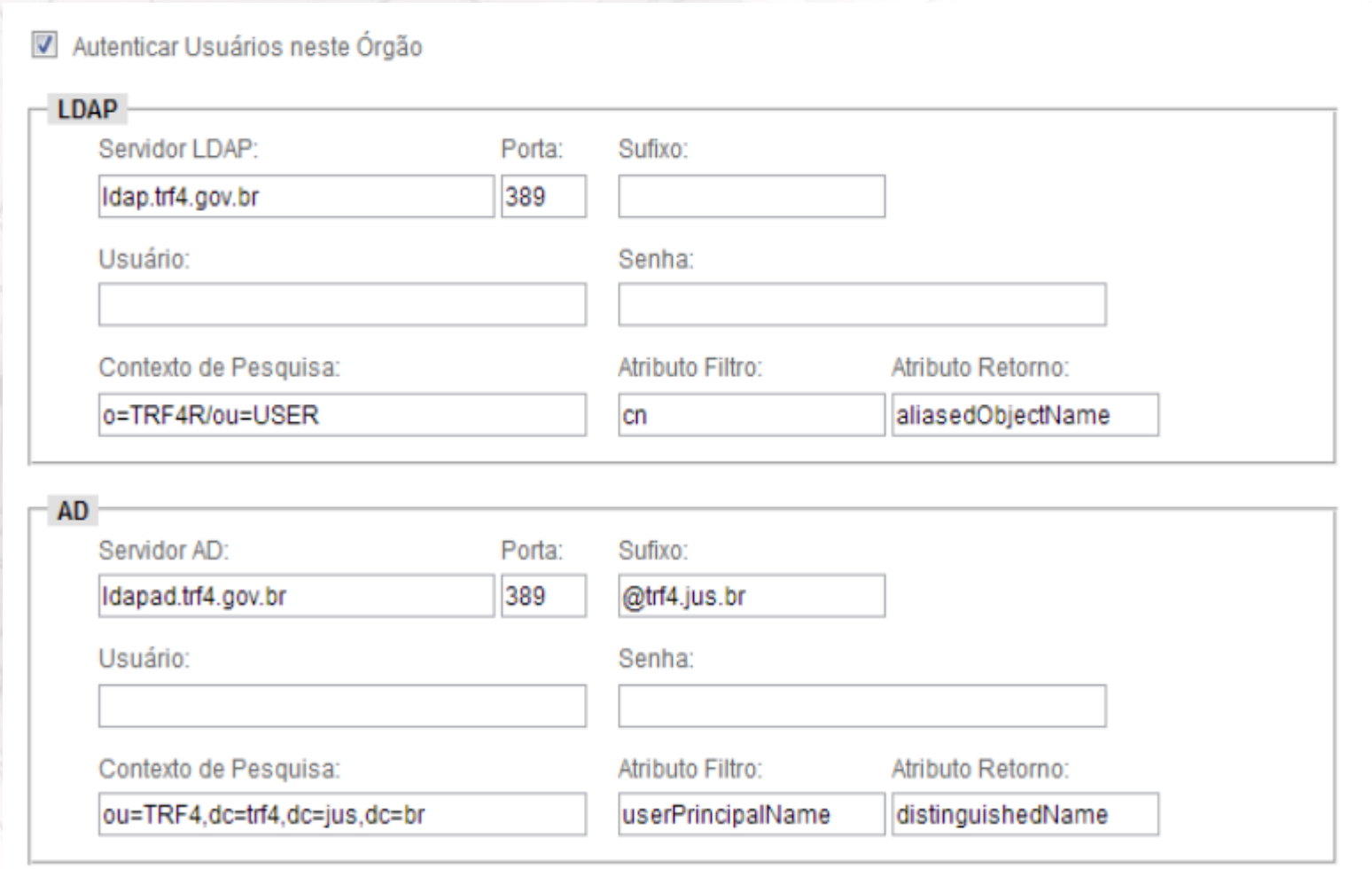
- Máquina Virtual (VMWare)
- Sistema Operacional: **Red Hat Enterprise Linux 7.1**
- Memória: **8 GB**
- Disco: **50 GB**
- CPUs: **2**
- Serviços:
  - **Apache 2.4.6**
  - **PHP 5.6.5**
  - **Aplicação SEI**
  - **MySQLi 5 ● MSSQL/FreeTDS 0.95 ● OCI8 2.0.5**
  - **Fontes True Type**

Mecanismos de Autenticação e Autorização

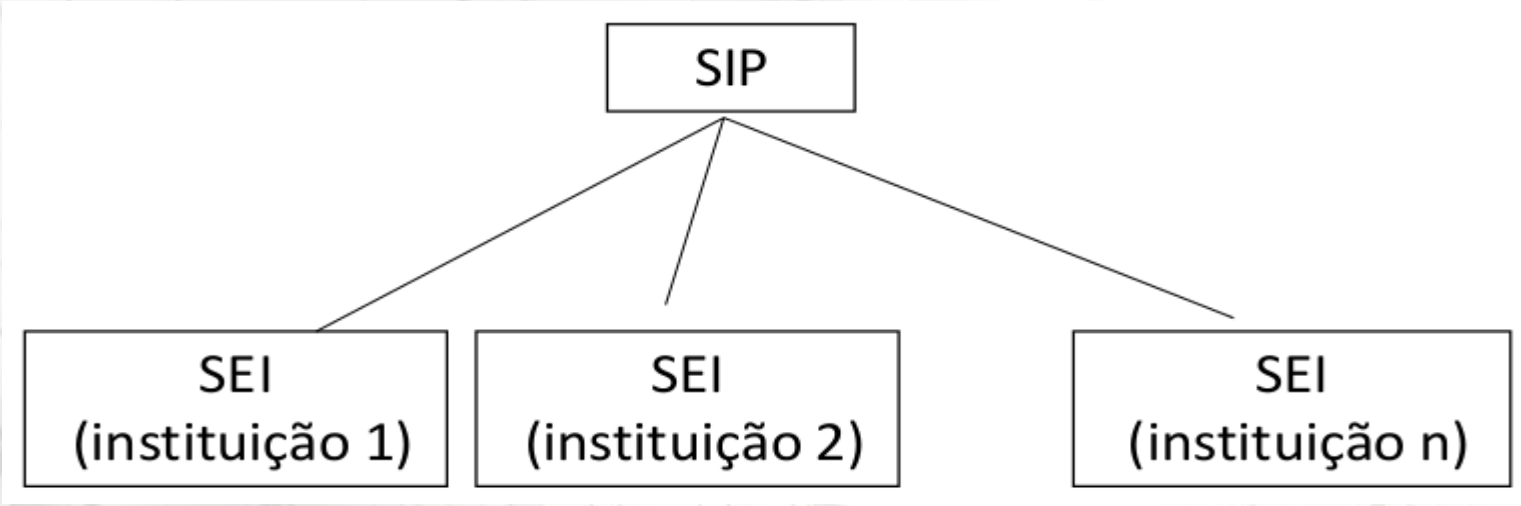
SIP (Sistema de Permissões)

- Autenticação via LDAP/AD ou personalizada;
- Perfis (conjunto de recursos e itens de menu);
- Administrador SIP, Administrador de Sistema,
- Coordenador de Perfil, Coordenador de Unidade;
- Cadastro de Usuários e Unidades (manual ou deve
- ser implementada rotina para replicação);
- Hierarquia de unidades.

SIP – Configuração LDAP



SIP – OPÇÃO A



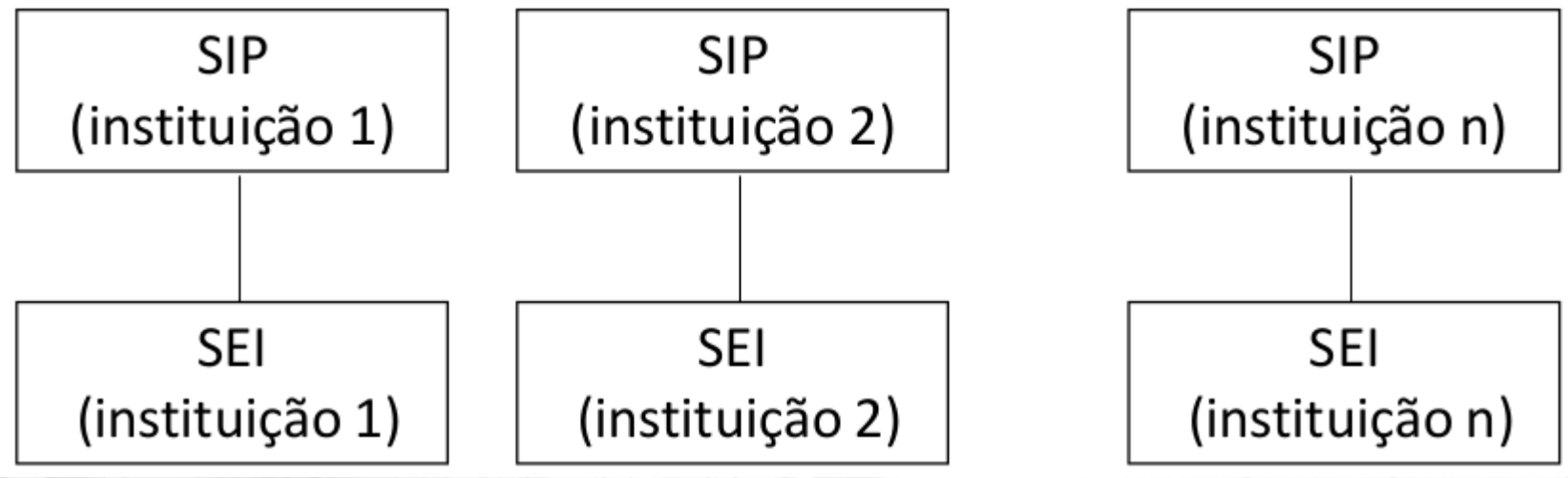
Vantagens

- Maior facilidade para integrar posteriormente;

Desvantagens

- Maior dependência do SIP;
- Necessidade de adaptações no SIP.

SIP – OPÇÃO B



Vantagens

- Nenhuma adaptação necessária no SIP;
- Mais independência dos órgãos no caso de falhas;

Desvantagens

- Mais trabalho para integrar posteriormente.

Mecanismos de segurança

- Links assinados em todo o sistema
- Hash de documentos do repositório de arquivos
- Armazenamento do arquivo p7s para assinaturas digitais
- CRC do conteúdo do documento nas assinaturas (CRC32B)
- Captcha
- Validação Online
- Usado na página de validação

Assinatura Digital

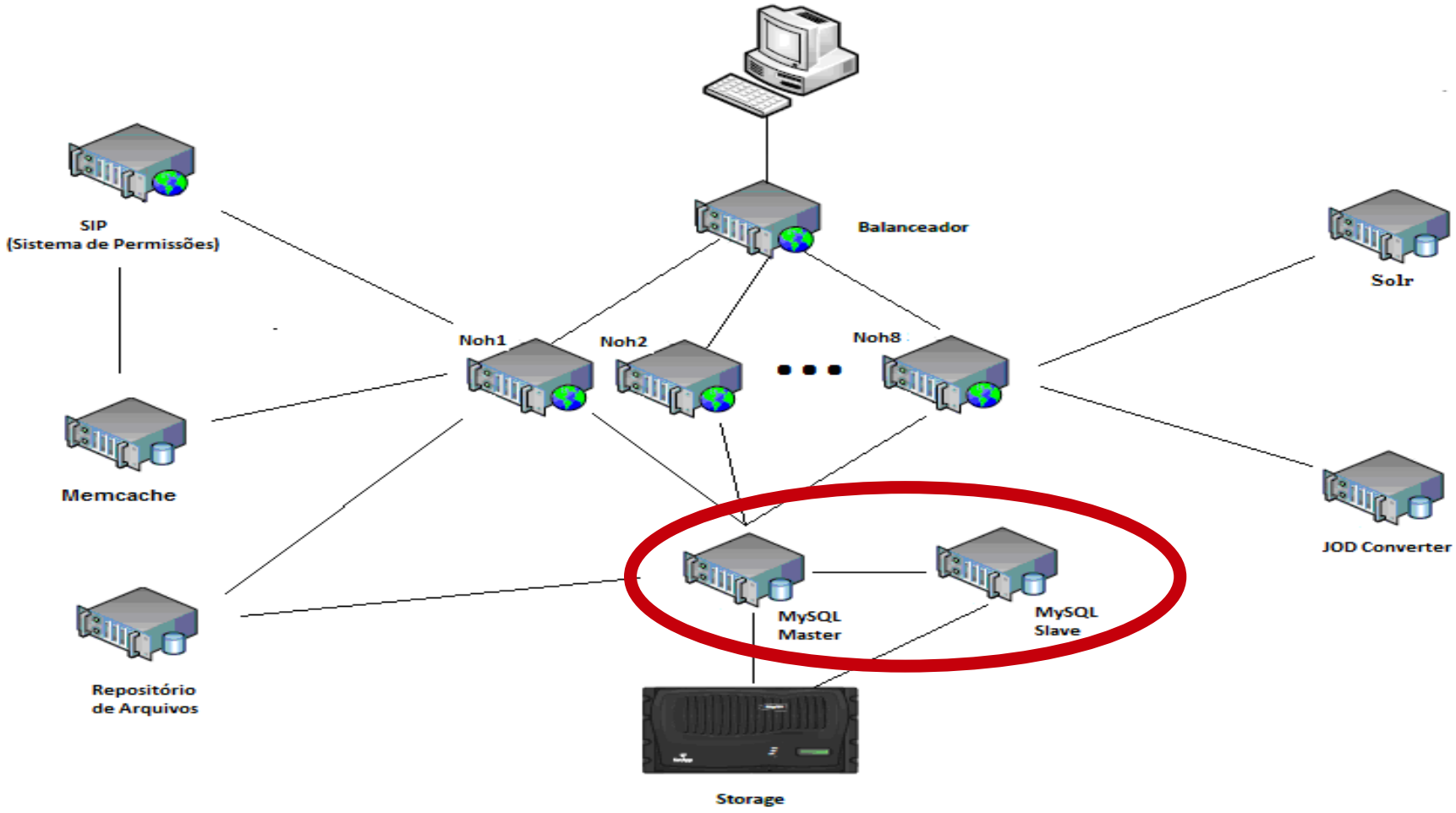
Applet Java

- BouncyCastle * Criptografia
- Axis * Web-Services
- Swing * Interface
- Log4j * Log
- Acessando o certificado com java.security.cert

Aceita certificados ICP-Brasil tipos A1 e A3

Gera arquivo p7s (PKCS#7 detached)

Infraestrutura de Hardware Sugerida



Infraestrutura de Hardware Sugerida

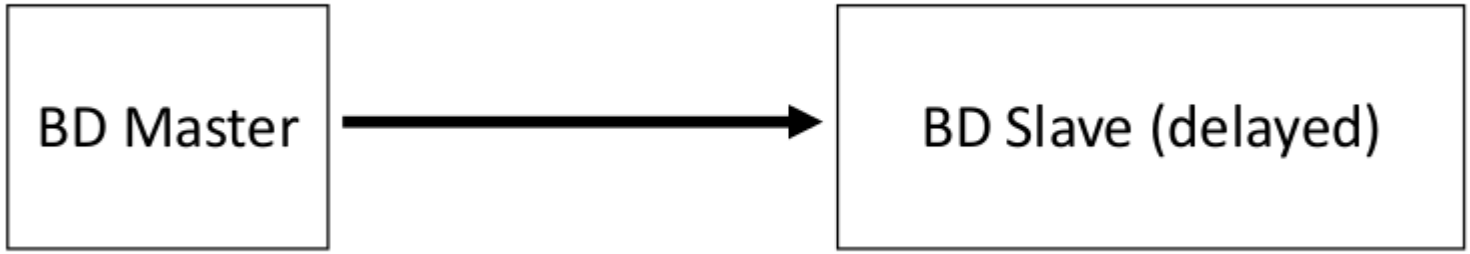
MySQL Master

- Sistema Operacional: **Red Hat Enterprise Linux 7.1**
- Memória: **128 Gb**
- CPUs: **2 x 10 núcleos**
- Serviços: **MySQL Enterprise Edition 5.6**

MySQL Slave

- Sistema Operacional: **Red Hat Enterprise Linux 7.1**
- Memória: **48 GB**
- CPUs: **2 x 4 Núcleos**
- Serviços: **MySQL Enterprise Edition 5.6**

Replicação e Backup



Após atualização dos logs inicia o backup dos slaves:

1º) Base SEI

2º) Base SIP

3º) Repositório de arquivos

Qual Banco de Dados Utilizar?

Microsoft® SQL Server®

ORACLE®

Base de Referência Poder Executivo

A Base de Referência do Poder Executivo facilita todo este trabalho de configuração, pois a sua instalação traz estas definições nativamente

Configuração Aplicadas

- Plano de Classificação
- Tipos de Processos (Atividades-Meio)
- Máscara Número Único de Protocolo (NUP)
- Modelos e Tipos de Documentos
- Hipóteses Legais de restrição de acesso
- Extensões de arquivos permitidas (PING)
- Listas de municípios e de países revisadas

Backup e Armazenamento

- Item **absolutamente crítico** em um sistema de processos eletrônicos
- Falhas = potencial desastre administrativo
- Modelo de backup que garanta o princípio da máxima disponibilidade da informação
- Restore rápido e confiável
- Acesso aos dados de backup: Respeitar ao sigilo de cada processo e documento (Decreto n°7.724/2012)

Backup e Armazenamento

- Orientações Gerais
- Dados a serem protegidos
- Estratégias de backup
- Período de retenção dos dados
- Local de armazenamento
- Monitoramento da rotina de backup
- Testes de recuperação do sistema

Orientações Gerais

- Documentação detalhada dos procedimentos
- Testes periódicos de restauração
- Definição de prazo de retenção com a área arquivística
- Backup off-site
- Aplicação da Política de Segurança da Informação
- Insumos do backup
- Mídias defeituosas

Dados a Serem Protegidos

Banco de dados do SEI

Utilizado recursos nativos de replicação de dados do SGBD

Banco de dados do SIP

Utilizado recursos nativos de replicação de dados do SGBD

Documentos Externos

Sincronização de dados periódica entre o servidor de NFS do ambiente de produção do SEI e uma rede de apoio

Serviço de Autenticação (LDAP)

Sincronização periódica do dump das bases de usuários do LDAP

Estratégias de Backup - Considerações

- Quantidade de informação que pode ser perdida
- Tempo para os serviços estarem novamente ativos
- Janela de tempo disponível para as rotinas de backup
- Orçamento disponível para a solução de backup
- Período de tempo de retenção dos dados

Sugestões

- Replicação dos dados
- Armazenamento de Logs Transacionais
- Snapshot das máquinas virtuais
- Backup incremental
- Backup full

Local de Armazenamento

- Armazenamento *off-site* (local remoto)
- Segurança no local para impedir acesso indevido
- (Decreto n°7.724/2012)
- Rápido acesso aos dados em caso de recuperação
- Uso de mídia apropriada

Monitoramento

- Utilização de ferramenta para monitoramento
  - Zabbix, Nagios, Zenoss, Cacti, etc.

- Serviços a monitorar:
  - Backup do banco de dados
  - Sincronização de arquivos externos
  - Snapshots dos servidores

Nagios®

ZABBIX

zenoss
Own IT.

Parametrizações Importantes

SEI_TAM_MB_DOC_EXTERNO

- Deverá refletir o tamanho máximo permitido pelo sistema
- Necessário configurar os parâmetros **post_max_size** e **upload_max_filesize**

SEI_TIPO_AUTENTICACAO_INTERNA

- 1 - autentica com login ou certificado
- 2 - somente login
- 3 - somente certificado

SEI_TIPO_ASSINATURA_INTERNA

- 1 - autentica com login ou certificado
- 2 - somente login
- 3 - somente certificado

Parametrizações Importantes

SEI_HABILITAR_AUTENTICACAO_DOCUMENTO_EXTERNO

- 0 - ninguém
- 1 - unidades de protocolo
- 2 - todas as unidades

SEI_HABILITAR_NUMERO_PROCESSO_INFORMADO

- 0 - ninguém
- 1 - libera para unidades de protocolo
- 2 - todas as unidades

SEI_HABILITAR_HIPOTESE_LEGAL

- 0 - desabilitado
- 1 - opcional
- 2 - obrigatório

Gargalos Eventuais já observados

Crescimento Excessivo do Banco de Dados

- Configuração do mecanismo de auditoria

Crescimento Excessivo do Repositório de Arquivos

- Configuração de Ferramentas de Conversão para PDF
- Configuração de Scanners e Multifuncionais
- Seguir Orientações sobre Digitalização de Documentos

Latência entre Servidores e Aplicação e Repositório de Arquivos

- Avaliar taxa de transferência entre estes dois nós infraestrutura
-

PEN

PROCESSO ELETRÔNICO NACIONAL

processo.eletronico@planejamento.gov.br

planejamento.gov.br/pensei

SECRETARIA DE GESTÃO

MINISTÉRIO DO PLANEJAMENTO, DESENVOLVIMENTO E GESTÃO

BRASIL GOVERNO FEDERAL