



Administradores de Guardium



Guardium®

Perallis IT Innovation
Soluções em Armazenamento de dados
www.perallis.com
contato@perallis.com
+55 19 3203-1002

Conteúdo

SOBRE ESTE CURSO.....	6
PÚBLICO-ALVO.....	6
OBJETIVO.....	6
PRÉ-REQUISITOS.....	7
AUTORES.....	7
1 INTRODUÇÃO.....	8
1.1 INFRAESTRUTURA DO GUARDIUM.....	9
1.1.1 ESPELHAMENTO DE PORTA (PORT MIRRORING).....	11
1.1.2 NETWORK TAP.....	12
1.2 SOFTWARE TAP (S-TAP).....	13
1.2.1 ARQUITETURA DO S-TAP.....	14
1.2.2 OPÇÕES DE ARQUITETURA DO S-TAP.....	15
OPÇÃO DE CONFIGURAÇÃO DO S-TAP COM FAILOVER.....	16
OPÇÃO DE CONFIGURAÇÃO DO S-TAP COM LOAD BALANCE.....	19
OPÇÃO DE CONFIGURAÇÃO DO S-TAP COM GRID.....	19
1.2.3 ARQUITETURA DO CAS.....	20
1.3 ARQUITETURA DO COLLECTOR.....	21
1.4 CENTRAL MANAGER E AGGREGATOR.....	21
1.4.1 AGGREGATOR.....	21
1.4.2 FUNCIONALIDADES DO CENTRAL MANAGER.....	22
1.4.3 CENÁRIOS DE IMPLEMENTAÇÃO.....	23
1.4.3.1 CENÁRIO GERAL.....	24
1.4.3.2 CENÁRIO AGGREGATOR E CENTRAL MANAGER.....	24
1.4.3.3 CENÁRIO AGGREGATOR DEDICADO.....	25
1.4.3.4 CENÁRIO CENTRAL MANAGER DEDICADO.....	25
1.5 COMO REGISTRAR UM MANAGEMENT UNIT.....	27
1.5.1 IMPLEMENTANDO UM CENTRAL MANAGER.....	27
1.5.2 IMPLEMENTANDO UM CENTRAL MANAGER NUMA NOVA INSTALAÇÃO.....	27
1.5.2.1 FAÇA UMA MÁQUINA SER O CENTRAL MANAGER.....	27
1.5.2.2 USE O MESMO SHARED SECRET.....	28
1.5.2.3 REGISTRANDO UNIDADES.....	28
1.5.2.4 REGISTRANDO UMA UNIDADE A PARTIR DO CENTRAL MANAGER.....	28
1.5.2.5 REGISTRANDO A PARTIR DA UNIDADE GERENCIADA.....	29
1.5.2.6 AGRUPANDO UNIDADES GERENCIADAS.....	30
1.5.3 IMPLEMENTANDO UM CENTRAL MANAGER NUMA INSTALAÇÃO EXISTENTE.....	31
1.5.4 SE A UNIDADE DE CENTRAL MANAGER ESTÁ INDISPONÍVEL.....	31
1.5.5 COMO REPLICAR AS CONFIGURAÇÕES DO CENTRAL MANAGEMENT PARA OS COLLECTORS.....	32

2 INSTALANDO O GUARDIUM.....	34
2.1 PRÉ-REQUISITOS.....	35
2.2 CONFIGURAÇÃO DE IP E MÁSCARA.....	38
2.3 SERVIDOR DNS.....	39
2.4 SERVIDOR SMTP.....	40
2.5 HOST E DOMÍNIO.....	40
2.6 CONFIGURANDO TIME ZONE, DATA E TEMPO.....	41
2.7 CONFIGURAR INITIAL UNIT TYPE.....	42
2.8 RESET ROOT PASSWORD.....	42
2.9 VALIDANDO TODAS AS CONFIGURAÇÕES.....	43
2.10 REINICIANDO O SISTEMA.....	43
2.12 VERIFICAR SE A INSTALAÇÃO FOI FEITA COM SUCESSO.....	44
2.13 GERENCIAMENTO DE LICENÇAS.....	44
2.14 INSTALAÇÃO DE PATCHES (CLI).....	45
3 INSTALAÇÃO GIM E MÓDULOS.....	47
3.1 INSTALAÇÃO GIM.....	48
3.1.1 INSTALANDO O CLIENTE GIM NO UNIX/LINUX.....	48
3.1.2 INSTALANDO O CLIENTE GIM NO WINDOWS.....	50
3.1.2 VERIFICANDO QUE O CLIENTE GIM FOI REGISTRADO NO SERVIDOR GIM.....	51
3.2 INSTALAÇÃO S-TAP.....	52
3.2.1 PREPARANDO PARA INSTALAR E CONFIGURAR O S-TAP USANDO GIM.....	52
3.2.1 INSTALANDO E CONFIGURANDO O S-TAP USANDO GIM (UNIX/LINUX).....	55
3.2.1 INSTALANDO E CONFIGURANDO O S-TAP USANDO GIM (WINDOWS).....	58
3.3 CONFIGURAÇÃO DO A-TAP.....	59
4 DATABASE AUTO DISCOVERY.....	61
4.1 O QUE É O AUTO DISCOVERY.....	62
4.1.1 POR QUE USAR O AUTO DISCOVERY.....	62
4.1.2 DEFININDO UM PROCESSO DE AUTO DISCOVERY.....	63
4.2 DATABASE INSTANCE DISCOVERY.....	65
5 USUÁRIOS E PERMISSÕES.....	67
5.1 USUÁRIOS DE ACESSOS DEFAULT.....	68
5.2 AUTORIZAÇÃO X AUTENTICAÇÃO.....	68
5.3 CONFIGURAR A AUTENTICAÇÃO.....	69
5.4 SEGURANÇA EM NÍVEL DE DADOS.....	70
5.5 CONTAS.....	70

5.5.1 CRIANDO UMA CONTA DE USUÁRIO MANUALMENTE.....	71
5.6 IMPORTANDO AS CONTAS POR LDAP.....	72
5.7 MODIFICANDO A ROLE DE UM USUÁRIO.....	73
5.8 ROLE CUSTOMIZADA.....	74
5.9 ADICIONANDO UMA ROLE.....	74
6 COMANDOS CLI.....	76
6.1 ACESSANDO O CLI.....	77
6.1.1 ACESSO SSH.....	77
6.1.2 CLI LOGIN.....	77
6.2 COMANDOS CLI – CONFIGURAÇÃO E CONTROLE.....	78
6.3 COMANDOS DE INSTALAÇÃO COLLECTOR E AGGREGATOR.....	81
6.3.1 CONFIGURAÇÃO DE REDE.....	81
6.4 COMANDOS CLI.....	85
7 S-GATE.....	88
7.1 O QUE É S-GATE.....	89
7.2 MODOS.....	89
7.2.1 OPEN MODE.....	89
7.2.2 CLOSED MODE (S-TAP FIREWALL MODE).....	90
7.3 CONFIGURAÇÕES.....	91
7.4 AÇÕES.....	93
7.4.1 USANDO AÇÕES DO S-GATE EM REGRAS DE SEGURANÇA.....	94
7.4.2 CONSIDERAÇÕES DE FUNCIONALIDADE.....	95
8 CAS – CONFIGURATION AUDIT SYSTEM.....	96
8.1 CONFIGURAÇÃO DO SISTEMA DE AUDITORIA.....	97
8.2 CONFIGURAÇÃO PARA MONITORAMENTO.....	98
8.3 PRÉ REQUISITOS.....	98
8.4 INSTALANDO O CAS.....	99
8.5 PARÂMETROS DO CAS.....	100
9 SELF-MONITORING.....	103
9.1 FERRAMENTAS PARA AUTO-MONITORAÇÃO.....	104
9.2 MONITORES PRÉ-DEFINIDOS.....	106
9.2.1 ALERTAS PRÉ-DEFINIDOS DE AUTO-MONITORAÇÃO DE LIMIAR.....	107
9.2.2 CONFIGURANDO E ATIVANDO ALERTAS PRÉ-DEFINIDOS.....	108
9.3 RELATÓRIOS.....	112

9.4 ALERTA DE SNIFFER RESTART.....	114
9.5 ALTO USO DE CPU.....	116
9.6 ALERTAS DE USO DE DISCO DE BANCO DE DADOS.....	118
9.6.1 ALERTA DE ESPAÇO EM DISCO DO AGGREGATOR.....	118
9.6.2 ALERTA DE ESPAÇO EM DISCO DO COLLECTOR.....	120
9.7 ALERTAS DE S-TAPS INATIVOS.....	122
9.8 ALERTAS DE AUSÊNCIA DE TRÁFEGO.....	122
9.9 VISUALIZAÇÃO ONLINE DE LOGS.....	122
9.10 S-TAP STATISTICS.....	124
9.11 DIAG.....	126
9.12 APLICAÇÃO DE PATCHES.....	128
10 BACKUP E RESTORE.....	129
10.1 BACKUP.....	130
10.1.1 STORAGE LOCAL BACKUP (CENTERA OU TSM).....	132
10.2 RESTORE.....	133
10.3 RESTORE ESPECÍFICO.....	134
11 PURGE E ARCHIVING.....	136
11.1 PROCESSO DE PURGE.....	137
11.2 PROCESSO DE ARCHIVE.....	138
11.3 CONFIGURAÇÃO PURGE.....	140
11.4 CONFIGURAÇÃO ARCHIVE.....	140
11.4.1 CONFIGURAÇÃO AGGREGATOR.....	140
11.4.1 CONFIGURAÇÃO COLLECTOR.....	142
12 IMPORT E EXPORT.....	143
12.1 IMPORTAÇÃO E EXPORTAÇÃO DE DADOS.....	144
12.1.1 CONFIGURAÇÃO DA IMPORTAÇÃO DE DADOS.....	144
12.1.2 CONFIGURAÇÃO DA EXPORTAÇÃO DE DADOS.....	145
13 DOCUMENTAÇÃO.....	147
13.1 HELP BOOK.....	148
13.2 KNOWLEDGE CENTER.....	149

SOBRE ESTE CURSO

PÚBLICO-ALVO

O **Curso Infosphere Guardium para Administradores** é voltado para profissionais de TI que pretendem tornar-se administradores da ferramenta Infosphere Guardium da IBM.

OBJETIVO

Preparar profissionais de TI para trabalharem com a ferramenta Infosphere Guardium. Ao final deste curso os alunos deverão ser capazes de:

- Compreender a arquitetura e o funcionamento do Guardium
- Instalar o Guardium e seus correspondentes módulos
- Descobrir novos bancos de dados e instâncias
- Criar e definir roles para usuários
- Executar comandos do CLI
- Gerar relatórios do CAS
- Fazer automonitoramento
- Fazer backup e restore
- Fazer import e export
- Fazer purge e archiving