



Curso Infosphere Guardium para Usuários



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 MAPA DO GUI.....	8
1.1 VISÃO GERAL DO PORTAL.....	9
1.2 ACESSO.....	9
1.3 ABAS.....	10
1.3.1 SYSTEM VIEW.....	11
1.3.2 ADMINISTRATION CONSOLE.....	11
1.3.3 TOOLS.....	13
1.3.4 DAILY MONITOR.....	14
1.3.5 GUARDIUM MONITOR.....	15
1.3.6 TAP MONITOR.....	15
1.3.7 INCIDENT MANAGEMENT.....	16
1.3.8 SEARCH.....	17
1.3.9 VIEW.....	18
1.3.10 QUICK START.....	19
1.3.11 MONITOR/AUDIT.....	19
1.3.12 DISCOVER.....	20
1.3.13 ASSESS/HARDEN.....	21
1.3.14 COMPLY.....	22
1.3.15 PROTECT.....	22
2 CONCEITOS DE AUDITORIA GUARDIUM.....	23
2.1 REQUISITOS DE AUDITORIA.....	25
2.2 REGULAMENTAÇÕES.....	28
2.3 MONITORAMENTO DE USUÁRIO PRIVILEGIADO X REGULAMENTOS.....	29
2.4 CATEGORIAS DE AUDITORIA.....	30
2.4.1 USUÁRIO PRIVILEGIADO.....	31

2.4.2 MONITORAMENTO DE OBJETOS SENSÍVEIS.....	33
2.4.3 MONITORAMENTO ABRANGENTE.....	34
3 CLASSIFICAÇÃO DE DADOS SENSÍVEIS.....	36
3.1 INFORMAÇÃO SENSÍVEL.....	37
3.2 FUNCIONAMENTO DA CLASSIFICAÇÃO.....	37
3.3 POLÍTICA DE CLASSIFICAÇÃO E PROCESSO DE CONSTRUÇÃO.....	38
3.4 CLASSIFICAÇÃO DE AÇÕES.....	43
3.5 POLÍTICA DE CLASSIFICAÇÃO.....	43
3.6 DEFININDO OS PROCESSOS DE CLASSIFICAÇÃO.....	47
3.7 RELATÓRIO DE CLASSIFICAÇÃO.....	50
3.8 BENEFÍCIOS.....	52
4 POLÍTICAS DE SEGURANÇA.....	54
4.1 POLÍTICAS DE SEGURANÇA, REGRAS E AÇÕES.....	55
4.2 CRIAÇÃO DE UMA NOVA POLÍTICA DE SEGURANÇA.....	56
4.2.1 AÇÕES.....	59
4.2.2 COMPORTAMENTOS DE AUDITORIA (LOGGING) PADRÃO.....	60
4.2.3 AÇÕES BÁSICAS DE LOG.....	60
4.2.3 AÇÕES DE LOG DETALHADAS.....	61
4.2.4 AÇÕES DE IGNORE.....	63
4.2.5 BASELINE.....	63
4.2.6 INSTALANDO POLÍTICAS DE SEGURANÇA.....	64
4.2.7 CONFIGURAÇÃO DO INSPECTION ENGINE.....	65
4.3 COMO FAZER BLOQUEIO E DEIXAR EM QUARENTENA.....	66
4.3.1 O QUE É QUARENTENA.....	66
4.3.2 REGRAS DE POLÍTICA DE SEGURANÇA.....	66
4.3.3 QUARENTENA AUTOMÁTICA A PARTIR DE RELATÓRIOS.....	68
5 RELATÓRIOS DE VULNERABILIDADES.....	70
5.1 O QUE É O RELATÓRIO DE VULNERABILIDADES.....	71
5.2 POR QUE É IMPORTANTE?.....	71
5.3 COMO FUNCIONA.....	72
5.3.1 TESTES PRÉ-DEFINIDOS: EXEMPLOS DE VULNERABILIDADES.....	73
5.4 CRIANDO UM RELATÓRIO DE VULNERABILIDADES.....	74
5.4.1 REPORTANDO.....	76
6 RELATÓRIO DE TITULARIDADE.....	78
6.1 TITULARIDADE.....	79

6.2 RELATÓRIO DE TITULARIDADE GUARDIUM.....	79
6.3 PRÉ REQUISITOS.....	80
6.4 PASSOS DE CONFIGURAÇÃO.....	81
6.5 CONFIGURAÇÕES AVANÇADAS.....	85
7 CONSTRUÇÃO DE RELATÓRIOS.....	87
7.1 RELATÓRIOS.....	88
7.2 ENTENDENDO A ESTRUTURA DOS RELATÓRIOS.....	89
7.2.1 DOMÍNIO.....	89
7.2.2 ENTIDADE PRINCIPAL.....	90
7.2.3 ATRIBUTOS.....	91
7.3 CONSTRUINDO RELATÓRIOS PRÉ-DIFINIDOS.....	92
8 ALERTAS.....	94
8.1 ALERTAS GUARDIUM.....	95
8.2 ALERTAS DE TEMPO REAL.....	96
8.3 CORRELATION ALERT.....	97
8.4 ASPECTOS DE UTILIZAÇÃO E FUNCIONAMENTO.....	97
9 REDACT.....	99
9.1 O QUE É REDACT?.....	100
9.1.1 PORQUE USAR REDACT?.....	100
9.1.2 COMO FUNCIONA?.....	101
9.1.3 CONSIDERAÇÕES.....	102
9.2 COMO FAZER.....	102
9.2.1 CRIE UM GRUPO PARA USUÁRIOS DO REDACT.....	102
9.2.2 ADICIONANDO MEMBROS AO GRUPO REDACT USERS.....	103
9.2.3 CRIE UMA POLÍTICA.....	104
9.2.4 INSTALE A NOVA POLÍTICA REDACT DEMO.....	105
9.2.5 TABELA EMPLOYEE ANTES E DEPOIS DO REDACT.....	106
10 APPLICATION USER IDENTIFICATION.....	107
10.1 O QUE É APPLICATION USER IDENTIFICATION?.....	108
10.1.1 ENTENDENDO O PROBLEMA.....	108
10.2 CRIANDO UMA APPLICATION USER IDENTIFICATION.....	108
10.2.1 A SOLUÇÃO DO GUARDIUM PARA O PROBLEMA.....	109
10.2.2 APPLICATION USER TRANSLATION.....	109
10.2.3 APPLICATION EVENTS API.....	110
10.2.4 STORED PROCEDURES.....	111

10.2.5 APPLICATION SERVER S-TAP.....	112
10.2.6 UID CHAINING.....	112

11 DOCUMENTAÇÃO..... 114

11.1 HELP BOOK.....	115
11.2 KNOWLEDGE CENTER.....	116