

Agilent OpenLab Server e OpenLab ECM XT

Guia de Administração

Avisos

Identificação do documento

Nº doc. D0035354pt B.00
EDIÇÃO 05/2024

Copyright

© Agilent Technologies, Inc. 2024

Nenhuma parte deste material pode ser reproduzida de qualquer forma ou por qualquer meio (incluindo armazenamento e recuperação eletrônica ou a tradução para outro idioma) sem autorização prévia por escrito da Agilent Technologies, Inc. de acordo com as leis de direitos autorais americanas e internacionais.

Agilent Technologies, Inc.
5301 Stevens Creek Blvd.
Santa Clara, CA 95051

Revisão do Software

Este guia é válido para a revisão 2.8 ou superior do programa Agilent OpenLab Server e OpenLab ECM XT até ser substituído.

Garantia

O material contido neste documento é fornecido "no estado em que se encontra" e está sujeito a alterações, sem aviso prévio em edições futuras. Além disso, com o máximo rigor permitido pelas leis aplicáveis, a Agilent isenta-se de responsabilidade em relação a garantias, expressas ou implícitas, em relação a este manual e a qualquer informação contida nele, incluindo mas não limitado as garantias implícitas de adequação comercial e adequação a um propósito específico. A Agilent não será responsável por erros ou por danos incidentais ou consequenciais relacionados ao fornecimento, ao uso ou ao desempenho deste documento ou de qualquer informação nele contida. Se a Agilent e o usuário possuírem um acordo por escrito em separado com os termos de garantia cobrindo o material neste documento que entrem em conflito com esses termos, os termos de garantia do documento em separado prevalecerão.

Licenças de tecnologia

O hardware e/ou software descrito(s) neste documento é/são fornecido(s) sob licença, podendo ser usado(s) ou copiado(s) somente de acordo com os termos dessa licença.

Legenda de direitos restritos

Direitos restritos ao governo dos EUA.
Os direitos de software e dados técnicos concedidos ao governo federal incluem apenas os direitos normalmente concedidos aos clientes usuários finais. A Agilent fornece esta licença comercial habitual relativamente a software e dados técnicos de acordo com a FAR 12.211 (Dados técnicos) e 12.212 (Software de computador) e, para o Departamento de Defesa, segundo a DFARS 252.227-7015 (Dados técnicos – Itens comerciais) e DFARS 227.7202-3 (Direitos relativos a software de computador comercial ou documentação de software de computador).

Avisos de segurança

CUIDADO

Um aviso de **CUIDADO** representa um perigo. Ele chama a atenção para um procedimento, prática ou algo semelhante que, se não forem corretamente realizados ou cumpridos, podem resultar em avarias no produto ou perda de dados importantes. Não prossiga após uma indicação de **CUIDADO** até que as condições indicadas sejam completamente compreendidas e atendidas.

AVISO

Um **AVISO** representa um perigo. Ele chama a atenção para uma prática, um procedimento operacional ou similares que, se não forem seguidos corretamente poderão resultar em lesões pessoais ou fatais. Não prossiga após uma indicação de **AVISO** até que as condições indicadas tenham sido totalmente compreendidas e atendidas.

Comunidade Agilent



Comunidade Agilent

Para obter respostas às suas dúvidas, junte-se a mais de 10.000 usuários na Comunidade Agilent. Analise os materiais de suporte selecionados e organizados por tecnologia de plataforma. Faça perguntas aos colegas e colaboradores do setor. Receba notificações sobre novos vídeos, documentos, ferramentas e webinars relevantes para o seu trabalho.

<https://community.agilent.com/>

Índice

1	Introdução e Visão Geral	7
	Arquitetura do Sistema do Servidor de Aplicativos OpenLab Server/ECM XT	8
	Navegador de Conteúdo	9
	Administração de Armazenamento	10
	Suporte ao CFR 21 Parte 11	11
2	Control Panel e Segurança	12
	Gerenciamento de Licença	13
	Recursos habilitados por licença	13
	FlexNet Publisher Suite	14
	Diagnósticos	15
	Relatórios administrativos	16
	Segurança	17
	Registro de Atividades do Sistema	17
	Provedor de autenticação	17
	Usuários, grupos e funções	18
	Política de segurança	20
	Reativar o Secure Storage após alterar o Servidor Host	22
3	Protegendo o Sistema	23
	Visão geral	24
	Infraestrutura geral de certificados	25
	Procedimento para Proteger Servidores do OpenLab Server/ECM XT	26
	Forçar o uso de LDAPS em vez de LDAP para consultar o Active Directory	26
	Impedir a comunicação de entrada do OpenLab Server/ECM XT pela porta 80	27
	Instalação e configuração de certificado comercial	27
	Gerar uma Solicitação de Assinatura de Certificado (CSR) usando OpenSSL	27
	Solicitar o certificado e reconfigurar o proxy reverso	28
	Reconfigurar as configurações do servidor e reativar	30
	Desabilitar TLS/SSL	31
	Cabeçalho do servidor	31
	Reiniciar o servidor	31

4 Manutenção 32

Manutenção de Rotina do Servidor 33

Atualizar estatísticas do banco de dados 33

Procedimentos de Manutenção do banco de dados PostgreSQL 33

Procedimentos de Manutenção do SQL Server 35

Monitorar utilização de recursos no servidor OpenLab Server/ECM XT 36

Melhores práticas adicionais 36

Domínio do Windows 37

Atualizar o Domínio, Nome de Usuário ou Senha de seu servidor 37

Ativar permissão de leitura para um usuário 37

Configurações do servidor 38

Arquivar 39

Etapa 1: Adicionar um local de armazenamento de acervo ao Secure Storage 39

Etapa 2: Configurar um agendamento para bloquear as pastas automaticamente 39

Etapa 3: Realocar pastas para o local de armazenamento de acervo 40

Exemplo: Configurar armazenamento automático de acervo de arquivos 40

5 Procedimentos de Backup e Restauração 41

Informações Importantes sobre Backup e Restauração 42

Usando o Amazon Web Services S3 como um local de backup 43

Criar um Plano de Recuperação de Desastres 44

Usar os Utilitários de Backup e Restauração 46

Backup do OpenLab Server/ECM XT Usando o Utilitário de Backup 47

Procedimentos para uso do Utilitário de Backup 49

Verificação do backup 52

Backup incremental de bancos de dados PostgreSQL 54

Configurar backup incremental usando a Ferramenta de Configuração Incremental 55

Configurar o diretório de dados personalizado do banco de dados PostgreSQL 56

Restaurar o OpenLab Server/ECM XT Usando o Utilitário de Restauração 57

Restaurar um sistema com banco de dados PostgreSQL ou Microsoft SQL 58

Reconfiguração durante a restauração 60

6	Procedimentos Manuais de Cold Backup e Restauração	62
	Procedimento Manual de Backup do Servidor de Aplicativos OpenLab Server/ECM XT	63
	Fazer um backup manual do sistema	63
	Procedimento Manual de Restauração do Servidor de Aplicativos OpenLab Server/ECM XT	68
7	Considerações sobre Hot Backup Manual	76
	Diretrizes de Backup	77
	Visão Geral	78
	Backup Manual do Banco de Dados	79
	Fazer backup dos bancos de dados	80
	Backup Manual do Content Store	81
	Backup Manual da Configuração do Servidor OpenLab Server/ECM XT	82
	Armazenar os Arquivos de Backup	83
	Restauração do Sistema	84
8	Alterações e Reconfigurações do Servidor	85
	Mover o Servidor de Aplicativos OpenLab Server/ECM XT para um Novo Sistema Operacional	86
	Reconfiguração do Servidor OpenLab Server/ECM XT	87
	Desativar o OpenLab Server/ECM XT	87
	Fazer alterações na infraestrutura	89
	Executar o Utilitário de Configuração do OpenLab Server	92
	Ativar o OpenLab Server/ECM XT	93
	Acrescentar repositório de arquivo ou conteúdo adicional	93
	Alterar a Senha do Shared Services	94
9	Apêndice	95
	Assistência de Vendas e Suporte	96

Arquitetura do Sistema do Servidor de Aplicativos OpenLab Server/ECM XT 8

Navegador de Conteúdo 9

Administração de Armazenamento 10

Suporte ao CFR 21 Parte 11 11

Este guia é destinado ao administrador do OpenLab Server/ECM XT. É necessário conhecimento administrativo prévio básico em sistemas de gerenciamento de banco de dados. Além disso, também é necessário familiaridade com Backup e Restauração do Windows.

Este guia fornece informações sobre procedimentos administrativos e de manutenção que devem ser seguidos para assegurar que o OpenLab Server/ECM XT permaneça estável e funcione bem com o tempo.

Fornecer também diretrizes para suporte ao CFR 21 Parte 11, utilizando o Control Panel para acessar recursos de controle do Shared Services, fazendo backups regulares do seu servidor e restaurando o servidor caso ocorra um desastre como uma falha de hardware no servidor.

As ferramentas mencionadas no documento são para demonstrar os conceitos. Se a sua organização tiver outras ferramentas padronizadas, você pode utilizá-las contanto que confirme que elas realizam tarefas idênticas.

Arquitetura do Sistema do Servidor de Aplicativos OpenLab Server/ECM XT

O software de aplicativos OpenLab Server/ECM XT está instalado em um servidor executando um sistema operacional do Microsoft Windows Server. Componentes adicionais, incluindo o OpenLab Shared Services e armazenamento seguro são automaticamente instalados na mesma máquina. O banco de dados e o armazenamento de arquivos são instalados na mesma máquina ou externamente, dependendo da topologia desejada. Consulte o Guia de Requisitos de Hardware e Software do OpenLab Server e ECM XT para obter as topologias e softwares compatíveis.

A alteração do domínio do servidor após a instalação exige que o Suporte Agilent seja consultado diretamente.

Máquinas-cliente que acessam o servidor OpenLab Server/ECM XT usam os seguintes componentes:

- **Cliente Web do Navegador de Conteúdo** – O OpenLab Server/ECM XT oferece uma interface de usuário de cliente fino baseada na Web que pode ser acessada utilizando um navegador da Web. A interface da Web fornece acesso às pastas e aos arquivos do armazenamento seguro.
- **Cliente Web da Administração de Armazenamento** – As funções de administrador para manter e gerenciar os locais de armazenamento são encontradas na interface da Web de Administração de Armazenamento. A partir desta interface, você pode adicionar locais de armazenamento, realocar arquivos, agendar o bloqueio de arquivos e realizar importações de arquivos em massa.
- **Control Panel** – O Control Panel é a interface de usuário que fornece acesso às funções administrativas utilizadas para gerenciar o servidor OpenLab Server/ECM XT e o Shared Services.

Navegador de Conteúdo

Use o cliente Web do Navegador de Conteúdo para gerenciar conteúdo de armazenamento seguro. A funcionalidade inclui:

- Exibir pastas e arquivos em uma "visualização em árvore"
- Pesquisar por conteúdo
- Organizar conteúdo
- Visualizar propriedades de arquivos e pastas
- Visualizar arquivos (com a licença premium do ECM XT)
- Assinar arquivos eletronicamente (com a licença premium do ECM XT)
- Criar links seguros para o conteúdo (com a licença premium do ECM XT)

Para acessar o cliente Web do Navegador de Conteúdo, execute uma das seguintes ações:

- Use o seguinte URL: `https://<OpenLab application server name>/openlab-storage/`
- A partir do menu Iniciar no servidor, vá para **Agilent Technologies > Navegador de Conteúdo**.

Para obter informações sobre como usar o Navegador de Conteúdo, consulte a ajuda do Navegador de Conteúdo.

Administração de Armazenamento

O cliente Web de Administração de Armazenamento oferece funções para gerenciar o armazenamento seguro. A funcionalidade inclui:

- Adicionar locais de armazenamento e designar um local de armazenamento principal
- Realocar arquivos para outro local de armazenamento imediatamente ou com base em agendamento
- Agendar o bloqueio automático de pastas e subpastas
- Importar conteúdo em massa para o armazenamento seguro

Para acessar a Administração de Armazenamento, execute uma das seguintes ações:

- Use o seguinte URL: <https://<OpenLab application server name>/openlab-storage-admin/>
- A partir do menu Iniciar no servidor, vá para **Agilent Technologies > Administração de Armazenamento**.

Para obter informações sobre como usar o cliente Web de Administração de Armazenamento, consulte a ajuda da Administração de Armazenamento.

Suporte ao CFR 21 Parte 11

O OpenLab Server/ECM XT armazena dados em conformidade com o CFR 21 Parte 11. Oferece armazenamento seguro de dados com controle de acesso e um registro de auditoria. Os arquivos de dados possuem versões para garantir a rastreabilidade e a integridade dos dados. Além disso, o ECM XT fornece assinaturas eletrônicas que permitem aos usuários aprovar os dados.

Gerenciamento de Licença 13

Recursos habilitados por licença 13

FlexNet Publisher Suite 14

Diagnósticos 15

Relatórios administrativos 16

Segurança 17

Registro de Atividades do Sistema 17

Provedor de autenticação 17

Usuários, grupos e funções 18

Política de segurança 20

Reativar o Secure Storage após alterar o Servidor Host 22

Use o Control Panel para acessar os recursos de controle dos Shared Services, como política de segurança e configuração central. Esses recursos são descritos mais detalhadamente neste capítulo.

Gerenciamento de Licença

Esse serviço inclui a administração de todas as licenças necessárias para o seu sistema.

Recursos habilitados por licença

Os recursos do software são habilitados com base na licença que você adquiriu e instalou. A **Tabela 1** exibe os recursos disponíveis com a licença Padrão do OpenLab Server e a licença Premium do OpenLab ECM XT.

Tabela 1. Recursos habilitados por licença

Recurso	Básica/Padrão (OpenLab Server)	Premium (ECM XT)
Navegador de Conteúdo	X	X
Baixar	X	X
Carregar	X	X
Copiar	X	X
Mover	X	X
Excluir	X	X
Assinatura Eletrônica		X
Bloquear e desbloquear	X	X
Pesquisa rápida	X	X
Pesquisa expandida		X
Criar pasta	X	X
Renomear pasta	X	X
Visualizar arquivos		X
Desfazer checkout	X	X
Visualizar o registro de atividades do arquivo	X	X
Visualizar os comentários do arquivo	X	X
Proteger cópia de link		X

FlexNet Publisher Suite

O OpenLab Server/ECM XT usa uma ferramenta terceirizada chamada *FlexNet Publisher Suite* da Flexera para gerenciar as licenças. Os componentes necessários do servidor de licenciamento são instalados por padrão no servidor de aplicativos.

O gerenciamento de licenças nos Shared Services requer a execução de um serviço adicional do Windows no servidor no qual você gerencia sua licença. Esse serviço do Windows é chamado de *Agilent OpenLab License Server*.

Antes de adicionar um arquivo de licença, é preciso adquirir a licença e gerar o arquivo de licença usando o SubscribeNet. Para obter mais informações sobre como gerar novos arquivos de licença, consulte o *Guia de Instalação do Agilent OpenLab Server e OpenLab ECM XT*.

O gerenciamento de licenças no Control Panel fornece as seguintes funções:

- É possível adicionar arquivos de licença ao servidor de licenças.
- É possível acessar o monitor de licenças e visualizar as propriedades de todas as licenças instaladas em qualquer servidor de licenças.
- É possível remover arquivos de licença do servidor de licenças. Isto pode ser útil se um arquivo de licença inválido foi adicionado.
- É possível visualizar ou alterar o servidor de licenças.
- É possível visualizar, copiar ou salvar o endereço MAC do servidor de licenças.
- É possível acessar a página da Web Entrega de Licenças e Software Eletrônico Agilent para obter uma licença.

Para obter mais informações sobre como adicionar arquivos de licença e visualizar as propriedades das licenças, consulte a Ajuda Online do Control Panel.

As propriedades a seguir são exibidas para as licenças instaladas:

- **Recurso:** Indica o tipo de licença utilizado.
- **Versão:** Se uma licença possuir versões, é possível visualizar o número da versão. Para licenças que não possuam versões, a versão será sempre exibida como 2.0.
- **Em uso (Disponível):** isso indica o número de licenças que estão sendo usadas atualmente e, entre parênteses, o número total de licenças. Com a estratégia de licenciamento do OpenLab Server/ECM XT, uma licença só é utilizada enquanto uma instância do software estiver sendo executada (consulte "[Gerenciamento de Licença](#)" na página 13).
- **Expiração:** Se a licença só for válida para um determinado período, a data de expiração será exibida.
- No painel **Alertas**, você é informado se o número de licenças disponíveis foi reduzido a zero para um recurso específico ou se tiver iniciado uma instância do software que precise de uma licença não disponível no momento.

Diagnósticos

A tela Diagnósticos permite acesso a vários relatórios e ferramentas para fins de diagnóstico:

- Executar ping no servidor do Shared Services.
- Criar um relatório, para o servidor do Shared Services, com informações sobre o sistema operacional, processadores, unidades de disco, processos, rede e conexões.
- Fazer download e acessar de forma central a todos os arquivos de registro/log, de rastreamento, etc., que são criados pelos módulos registrados.

Relatórios administrativos

Na tela Relatórios Administrativos, também é possível criar e exportar vários relatórios em XML ou PDF relacionados à configuração do sistema:

- **Relatório de Funções e Privilégios**

Descreve todas as funções definidas no sistema, incluindo detalhes de todos os privilégios incluídos em cada função.

- **Relatório de atribuição de funções de usuários e grupos**

Este relatório fornece uma visão geral de todos os direitos de acesso dos usuários e grupos aos instrumentos e projetos no sistema. Os usuários e grupos que não tiveram acesso garantido a instrumentos ou projetos não serão incluídos neste relatório.

Segurança

Registro de Atividades do Sistema

O Registro de Atividades do Sistema do Control Panel permite o acesso centralizado a todas as atividades do sistema. Ele contém informações sobre os vários eventos associados ao Shared Services e à gestão de arquivos e pastas. É possível filtrar a lista para que ela exiba apenas eventos de um determinado tipo, em um intervalo de tempo específico, criado por um certo usuário, ou que contenha uma determinada descrição.

Os seguintes tipos de eventos são registrados:

- Instrumento – Informações de registro fornecidas pelo hardware ou driver
- Configuração – Definições de configuração do sistema e da aplicação
- Segurança – Atividades de administração para adicionar usuários e modificar privilégios
- Acesso – Login/logoff e tentativas falhadas de login do usuário
- Geral – Atividade do sistema e da aplicação

Para obter mais informações sobre um evento, expanda a linha de interesse no visualizador do registro de atividades.

Provedor de autenticação

Os provedores de autenticação costumam fornecer a identidade dos usuários que iniciam sessão no sistema.

Durante a instalação, o OpenLab Server/ECM XT é automaticamente ativado e configurado utilizando uma autenticação interna com um usuário padrão, **admin**, e a senha **openlab**. No primeiro início de sessão, o sistema exigirá que o usuário troque a senha antes de continuar. Você poderá alterar o modo de autenticação, se necessário.

O OpenLab Server/ECM XT oferece suporte aos seguintes provedores de autenticação:

- **Interno**

Neste modo, as credenciais do usuário são armazenadas no banco de dados Shared Services. É solicitada a criação de uma conta de administrador para os Shared Services antes da configuração de outros usuários. Este é o único modo no qual é possível criar usuários dentro do sistema. Em todos os outros modos, só é possível mapear para usuários que existam em um sistema diferente.

- **Domínio do Windows**

Usuários existentes do Windows são importados para os Shared Services. A autenticação é feita por um Domínio do Windows dentro da empresa. O Shared Services usa apenas a identidade e senha dos usuários mapeados. As funções e os privilégios do OpenLab Server/ECM XT ainda são configurados com os Shared Services.

Usuários, grupos e funções

Os Shared Services permitem a atribuição de funções específicas a usuários ou grupos de usuários. Se você estiver gerenciando usuários dentro de um domínio do Windows, é possível mapear tais usuários para os Shared Services.

Os usuários podem ser membros de mais de um grupo. É preciso atribuir uma função específica a cada grupo. Também é possível atribuir funções a usuários separadamente. Porém, por questões de clareza, é altamente recomendada a atribuição de funções apenas para grupos.

As funções são equipadas com diversos privilégios específicos que definem o que os usuários podem visualizar ou fazer no Control Panel e no armazenamento seguro. A **Tabela 2** descreve as credenciais dos usuários.

Tabela 2. Credenciais de usuários

Valor	Descrição	Obrigatório
Nome	Nome de usuário para iniciar sessão no sistema	Sim
Descrição	Informações adicionais sobre o usuário (ex.: departamento, função, etc.)	Não
Senha	Senha do usuário; o tamanho mínimo da senha é definido na Política de Segurança	Sim
E-mail	Endereço de e-mail do usuário	Não
Nome completo	O nome completo do usuário	Não
Informações de contato	Informações gerais de contato (ex.: número de telefone, pager, etc.)	Não
Conta está desativada	Selecione a caixa de seleção para desativar o usuário. Usuários desabilitados não podem iniciar uma sessão. Os usuários podem ser desativados automaticamente após muitas tentativas de conexão sem sucesso. Se um usuário estiver desativado, é exibida uma mensagem correspondente em vez da caixa de seleção. Após um determinado tempo (consulte Duração do bloqueio da conta nas configurações de Política de Segurança), o usuário é habilitado de novo automaticamente.	Não
O usuário não pode alterar senha	O sinalizador indica se um usuário pode alterar sua própria senha. O sinalizador é falso por padrão (ou seja, usuários PODEM alterar suas senhas).	Não
O usuário deve alterar senha no próximo login	Se definido como verdadeiro, o usuário deverá alterar sua senha na próxima sessão. O sinalizador é definido automaticamente como falso após o usuário alterar a senha. Por padrão, o sinalizador é verdadeiro para novos usuários.	Não
Senha nunca expira	Se definida como verdadeira, o usuário nunca precisará trocar a senha.	Não
Participação em um Grupo	Atribua o usuário aos grupos relevantes.	Não
Participação na Função	Atribua funções diretamente ao usuário.	Não

Usuários

Se você utilizar o domínio do Windows como provedor de autenticação externo, não será possível criar usuários. Em vez disso, será necessário importar usuários existentes nos sistemas de autenticação. Uma função de pesquisa ajuda a encontrar usuários específicos no sistema de autenticação. No Control Panel, é possível gerenciar as funções para tais usuários externos, mas não as credenciais de usuários propriamente ditas, como nome de usuário e senha. Caso deseje remover um usuário externo, desative o mapeamento do usuário no Control Panel. O usuário ainda existirá no sistema de autenticação externo.

Grupos

Se um provedor de autenticação externo for usado, será possível importar os nomes dos grupos existentes no sistema externo ou criar novos grupos internos. Não existe limite para o número de grupos que podem ser mapeados ou criados.

É possível atribuir usuários aos grupos no sistema externo ou no Control Panel. Caso precise de mais atribuições de usuários que sejam relevantes apenas para o OpenLab CDS, crie-as no Control Panel. Caso contrário, basta importar os grupos e atribuir as funções necessárias a eles.

Se um grupo for excluído ou tiver seu mapeamento removido, os usuários que eram membros deste grupo não serão alterados.

Funções e privilégios

As funções são usadas para atribuir privilégios a um usuário ou globalmente a um grupo de usuários. O sistema possui uma lista de funções predefinidas que são instaladas como parte da instalação do sistema (consulte a [Tabela 3](#)). Cada função tem seus próprios privilégios atribuídos.

Ao atribuir privilégios a uma função, primeiro selecione o tipo de função necessária e, em seguida, os privilégios relacionados a esse tipo de função. Cada função só pode ter privilégios de um tipo específico de função. A única exceção é a função predefinida **"Tudo"**, que possui todos os privilégios de todos os tipos de funções. Os usuários ou grupos podem precisar de mais de uma função para desempenhar funções do sistema.

NOTA

É necessário que os usuários tenham o privilégio "Visualizar o registro de atividades" para visualizar o registro de atividades e todas as suas entradas. Durante uma atualização de versões anteriores, serão atribuídos a todos os usuários a função de "Acessar Registro de Atividades", para que os usuários não percam a funcionalidade. Após uma atualização, caso não queira que um usuário tenha acesso ao registro de atividades, você deverá remover essa função do usuário ou grupo.

Tabela 3. Privilégios do Secure Storage em funções predefinidas

Privilégios	Funções do Secure Storage	Tipo de função
Fazer check-in/check-out	<ul style="list-style-type: none"> Administrador de Secure Storage Colaborador de Secure Storage 	Projeto Projeto
Copiar arquivos/pastas	<ul style="list-style-type: none"> Administrador de Secure Storage Colaborador de Secure Storage 	Projeto Projeto
Criar/renomear pasta	<ul style="list-style-type: none"> Administrador de Secure Storage Colaborador de Secure Storage 	Projeto Projeto
Excluir arquivos/pastas	<ul style="list-style-type: none"> Administração do Secure Storage Excluir Conteúdo no Secure Storage 	Projeto Projeto
Baixar arquivos/pastas	<ul style="list-style-type: none"> Administrador de Secure Storage Aprovador do Secure Storage Arquivista de Secure Storage Colaborador de Secure Storage Visualizador de Secure Storage 	Projeto Projeto Projeto Projeto Projeto
Assinar arquivos eletronicamente	<ul style="list-style-type: none"> Aprovador do Secure Storage 	Projeto
Importar arquivos/pastas	<ul style="list-style-type: none"> Importador em Massa 	Administrativo
Bloquear arquivos/pastas	<ul style="list-style-type: none"> Administrador de Secure Storage Arquivista de Secure Storage 	Projeto Projeto

Tabela 3. Privilégios do Secure Storage em funções predefinidas

Privilégios	Funções do Secure Storage	Tipo de função
Gerenciar armazenamento de arquivos	<ul style="list-style-type: none"> Gestor de Locais de Armazenamento de Arquivos Gestor do Secure Storage 	Administrativo Administrativo
Gerenciar locais de armazenamento	<ul style="list-style-type: none"> Gestor de Configuração de Armazenamento Gestor de Locais de Armazenamento 	Administrativo Administrativo
Mover arquivos/pastas	<ul style="list-style-type: none"> Administrador de Secure Storage Colaborador de Secure Storage 	Projeto Projeto
Agendar bloqueio de arquivo	<ul style="list-style-type: none"> Gestor de Agendamento de Bloqueio 	Administrativo
Desfazer checkout para outros usuários	<ul style="list-style-type: none"> Administrador de Secure Storage 	Projeto
Desbloquear arquivos/pastas	<ul style="list-style-type: none"> Administrador de Secure Storage Arquivista de Secure Storage 	Projeto Projeto
Carregar arquivos/pastas	<ul style="list-style-type: none"> Administrador de Secure Storage Colaborador de Secure Storage 	Projeto Projeto
Visualizar o conteúdo	<ul style="list-style-type: none"> Administrador de Secure Storage Aprovador do Secure Storage Arquivista de Secure Storage Colaborador de Secure Storage Excluir Conteúdo no Secure Storage Visualizador de Secure Storage 	Projeto Projeto Projeto Projeto Projeto Projeto
Visualizar conteúdo de administração de armazenamento	<ul style="list-style-type: none"> Visualizar Conteúdo de Administração de Armazenamento 	Projeto

Política de segurança

Com o provedor de autenticação **Interno**, é possível definir os parâmetros descritos na **Tabela 2** no Control Panel. Com a autenticação por **Domínio do Windows**, só é possível definir o tempo de inatividade no Control Panel; todos os outros parâmetros são definidos pelo sistema externo. A **Tabela 4** descreve as configurações da política de segurança.

Tabela 4. Configurações da política de segurança

Configuração	Descrição
Tamanho mínimo da senha	Se os usuários alterarem suas senhas, eles terão de escolher uma senha com pelo menos o número de caracteres especificado. A configuração padrão é 5. Somente disponível para provedor de autenticação Interno .
Período de validade da senha (dias)	O valor padrão é de 0 dias. Esse período pode ser redefinido pelo administrador do sistema OpenLab. Quando o usuário tentar iniciar sessão após esse período, o sistema solicitará que ele altere a senha. O período de expiração é iniciado no momento da última alteração de senha ou da criação de um usuário com uma nova senha padrão. Somente disponível para provedor de autenticação Interno .
Número máximo de tentativas mal sucedidas de login antes do bloqueio da conta	Se um usuário tentar iniciar sessão utilizando credenciais de usuário inválidas um determinado número de vezes, o usuário será bloqueado por um certo intervalo de tempo (consulte abaixo Tempo de bloqueio de conta). Não é possível realizar login, mesmo com credenciais válidas de usuário. É possível definir o número de tentativas de login permitidas. A configuração padrão é 3. Somente disponível para provedor de autenticação Interno .

Tabela 4. Configurações da política de segurança

Configuração	Descrição
Tempo de bloqueio de conta (minutos)	Uma vez atingido o número máximo de tentativas de iniciar sessão sem sucesso, este é o intervalo de tempo que se deve esperar para tentar novamente. A configuração padrão é 5 min. Somente disponível para provedor de autenticação Interno .
Tempo de inatividade antes do bloqueio do aplicativo	Se o Control Panel ficar inativo por este período, a interface do usuário será bloqueada. Esta configuração também é usada para definir o bloqueio de sessão baseado em tempo na ChemStation. A configuração padrão é 10 min . Defina o valor para zero para nunca bloquear.
Assinatura única	Com a assinatura única ativada, o usuário não visualizará a tela de login do Control Panel. Disponível apenas para provedor de autenticação Domínio do Windows . A assinatura única não é suportada pelos back-ends do OpenLab ECM XT.

Reativar o Secure Storage após alterar o Servidor Host

Para reativar o Secure Storage após especificar um novo servidor host, use o procedimento a seguir.

- 1 Faça login no Control Panel. Se estiver atualizando, assegure-se de fazer login como um usuário que existia antes da atualização.
- 2 Clique em **Administração > Configuração do Sistema > Editar Configurações do Sistema**.
- 3 Na lista suspensa **Selecione outra opção da lista se desejar usar um tipo de armazenamento diferente**, selecione **Secure Storage** e, em seguida, clique em **Próximo**.
- 4 Selecione **Alterar o Servidor** e insira o URL do servidor do armazenamento seguro que deseja usar.
- 5 Clique em **Ativar**.
- 6 Na caixa de diálogo **Inserir credenciais**, digite seu Nome de usuário e Senha e (se necessário) selecione seu Domínio.
- 7 Clique em **OK**.
- 8 Você verá uma mensagem informando que o armazenamento seguro foi ativado com sucesso. Clique em **OK**.

3 Protegendo o Sistema

Visão geral 24

Infraestrutura geral de certificados 25

Procedimento para Proteger Servidores do OpenLab Server/ECM XT 26

Forçar o uso de LDAPS em vez de LDAP para consultar o Active Directory 26

Impedir a comunicação de entrada do OpenLab Server/ECM XT pela porta 80 27

Instalação e configuração de certificado comercial 27

Gerar uma Solicitação de Assinatura de Certificado (CSR) usando OpenSSL 27

Solicitar o certificado e reconfigurar o proxy reverso 28

Reconfigurar as configurações do servidor e reativar 30

Desabilitar TLS/SSL 31

Cabeçalho do servidor 31

Reiniciar o servidor 31

Utilize estes procedimentos para criar e instalar certificados para o conteúdo seguro e configurar o servidor de aplicativos OpenLab Server/ECM XT.

Visão geral

Os procedimentos desta seção se aplicam às topologias de servidor "all-in-one" e de 2 e 3 servidores.

Os certificados são necessários para habilitar a comunicação de rede segura e confiável entre os componentes do OpenLab – Servidor, Controladores de Instrumentos da Agilent (AICs) e Clientes. Os clientes podem confiar em um servidor se o servidor puder provar sua identidade usando um certificado válido. O OpenLab CDS conta com comunicação de rede segura via HTTPS. Na instalação, o Serviço de certificado do OpenLab no OpenLab Server gera uma Autoridade de Certificação Raiz do Agilent OpenLab, que emite certificados autoassinados para o OpenLab Server/ECM XT, AICs e Clientes do OpenLab CDS. Esses certificados permitem a comunicação confiável e segura de AICs e Clientes com o Servidor, pois o certificado OpenLab RootCA é instalado automaticamente no armazenamento de certificados do Windows da "máquina local" de cada máquina do OpenLab instalada neste servidor. Embora os certificados do OpenLab autoassinados tecnicamente permitam uma comunicação segura e confiável dentro dos ecossistemas OpenLab, os clientes podem optar por melhorar ainda mais o nível de confiança da comunicação segura usando certificados comerciais.

O uso de certificados comerciais para proteger o OpenLab Server pode oferecer as seguintes vantagens:

- Conformidade com sua política de segurança de TI.
- Os PCs sem o OpenLab CDS instalado ou outros dispositivos com recursos de navegação na Web configurados por sua TI confiarão no servidor OpenLab/ECM XT ao tentar acessar o armazenamento de conteúdo seguro através da interface da Web ou ao usar a interface da Web do Sample Scheduler.
- Alternar Clientes entre dois servidores OpenLab não exigirá a instalação manual do segundo certificado raiz do OpenLab Server/ECM XT no armazenamento de certificados do respectivo Cliente.
- Necessário para instalações em nuvem do OpenLab CDS, que não dependem apenas de redes VPN.

NOTA

No final de uma atualização com um certificado atualizado, o sistema estará no estado para uso de um certificado interno. Após a atualização, reconfigure e instale o certificado comercial.

Infraestrutura geral de certificados

- O cliente pode instalar certificados comerciais/personalizados se assim preferir, em vez dos certificados fornecidos pelo Agilent OpenLab. Os certificados comerciais são necessários para os sistemas na nuvem.
- O cliente é o proprietário dos seus certificados comerciais ou da infraestrutura de certificados. Os funcionários da Agilent apenas ajudarão a interpretar o manual e a instalar os certificados em um servidor OpenLab Server/ECM XT.
- Após a instalação dos certificados comerciais, os AICs e os Clientes devem ser registrados para o FQDN resolvível do OpenLab Server/ECM XT. Se esta abordagem foi usada na instalação inicial dos AICs/Clientes, não é necessário realizá-la novamente.
- O Reverse Proxy no AIC continuará usando o certificado interno da Agilent para permitir a comunicação do Cliente com o AIC.
- A instalação de novos AICs/Clientes resultará na geração de certificados internos do OpenLab para cada AIC/Cliente. Esses certificados são usados para comunicação segura do AIC/Cliente, por exemplo, proxy reverso/serviços de teste. O comportamento independe da topologia cliente-servidor.
 - O certificado OpenLab Root CA é instalado para cada Repositório de Autoridade de Certificação Raiz Confiável do AIC/Cliente.
- Consulte:
<https://www.ssl.com/guide/pem-der-crt-and-cer-x-509-encodings-and-conversions/>

Procedimento para Proteger Servidores do OpenLab Server/ECM XT

Use os procedimentos nesta seção na ordem apresentada para proteger seu sistema usando certificados.

Forçar o uso de LDAPS em vez de LDAP para consultar o Active Directory

Este procedimento força o Shared Services a usar o LDAPS em vez do LDAP após a instalação do OpenLab Server/ECM XT ao se comunicar com o controlador do domínio. Para implantações no Enterprise, essa etapa deve ser executada em cada servidor OpenLab Server/ECM XT.

Pré-requisitos

- Controladores de domínio existentes que suportam a conexão LDAPS
- O Shared Services se comunicará com os controladores de domínio do Active Directory através da Porta 636 do LDAPS

Procedimento

- 1 Interrompa o serviço **Agilent OpenLab Shared Services**.
- 2 Modifique o server.config.xml (caminho: <InstallationFolder>\Agilent Technologies\OpenLab Services\Server\server.config.xml) da seguinte forma:

Adicione ou atualize a seção AuthProviders da seguinte forma; adicione as configurações e especifique UseLdapsConnection como verdadeiro.

Original (LDAP):

```
server.config.xml
<AuthProviders>
  <WindowsDomain>
    <ReferralChasing>true</ReferralChasing>
  </WindowsDomain>
</AuthProviders>
```

Modificado (LDAPS):

```
server.config.xml
<AuthProviders>
  <WindowsDomain>
    <ReferralChasing>true</ReferralChasing>
    <UseLdapsConnection>true</UseLdapsConnection>
  </WindowsDomain>
</AuthProviders>
```

- 3 Reinicie o serviço **Agilent OpenLab Shared Services**.

Impedir a comunicação de entrada do OpenLab Server/ECM XT pela porta 80

Por padrão, o OpenLab Server/ECM XT escuta o tráfego de entrada na porta 80 e na 443. Ambas as portas são escutadas pelo OpenLab Reverse Proxy e as solicitações de entrada na porta 80 são automaticamente atualizadas para comunicação criptografada TLS segura através da porta 443. Se for necessário que a porta 80 não seja ocupada no seu sistema OpenLab Server/ECM XT, execute as seguintes etapas para escutar apenas na porta 443.

- 1 Abra um prompt de comando administrativo.
- 2 Execute o seguinte comando para fechar a porta 80:

```
"C:\Program Files (x86)\Agilent Technologies\OpenLab Platform\Reverse Proxy\rptool" SetUnsecureCommunication --switch off
```

Para reverter a etapa acima e reabrir a porta 80, use o comando a seguir:

```
"C:\Program Files (x86)\Agilent Technologies\OpenLab Platform\Reverse Proxy\rptool" SetUnsecureCommunication --switch on
```

Observações:

- Inserir apenas o URL do OpenLab Server/ECM XT no seu navegador com a porta 80 fechada pode impedir a chamada bem-sucedida da funcionalidade desejada a partir de um navegador da Web, pois ela pode tentar apenas uma conexão HTTP através da porta 80. Os aplicativos do OpenLab não são impactados.
- Por padrão, a porta 80 está fechada nos AICs do OpenLab CDS.
- O Reverse Proxy não é instalado nos clientes do OpenLab CDS.

Instalação e configuração de certificado comercial

Os certificados comerciais são suportados apenas nas topologias padrão do OpenLab Server/ECM XT. Os pontos de entrada do sistema Enterprise são protegidos por um certificado comercial no balanceador de carga e pelas configurações de segurança do balanceador de carga usado. Os nós individuais de um sistema Enterprise continuarão usando os certificados emitidos OpenLab Root CA em seus respectivos OpenLab Reverse Proxy.

Use os procedimentos nesta seção para gerar uma solicitação de assinatura de certificado e a chave privada para o OpenLab Server/ECM XT.

Gerar uma Solicitação de Assinatura de Certificado (CSR) usando OpenSSL

- 1 Abra um prompt de comando administrativo.
- 2 Crie um diretório de trabalho em seu servidor para permitir uma melhor rastreabilidade. O exemplo usará o diretório C:\https.

Exemplo:
mkdir c:\https

- 3 Defina a variável do ambiente para OpenSSL (instalado em conjunto com o Reverse Proxy).
`set OPENSSL_CONF=<InstallationFolder>\Agilent Technologies\OpenLab Platform\Reverse Proxy\Bin\openssl\ssl\openssl.cnf`
- 4 Para gerar o arquivo CSR e a chave não criptografada para o servidor onde o HTTPS será ativado
 - a Acesse o diretório OpenSSL.
`cd "<InstallationFolder>\Agilent Technologies\OpenLab Platform\Reverse Proxy\Bin\openssl\x64\bin"`
 - b Crie a solicitação de assinatura de certificado e a chave privada criptografada.
 Por exemplo:
`openssl req -new -passout pass:"<password>" -addext "subjectAltName = DNS:ecmxtserver.agilent.com" -out C:\https\ecmxtserver.agilent.com.csr -newkey rsa:2048 -keyout C:\https\ecmxtserver.agilent.com.key`
 O OpenSSL solicitará o Nome Comum (CN) do servidor OpenLab Server/ECM XT. Recomenda-se inserir o nome de domínio totalmente qualificado do servidor, por exemplo, ecmxtserver.agilent.com.
 - c Descriptografe a chave privada. (Não é necessário se o seu fornecedor de certificado emitir um .pfx.) Por exemplo:
`openssl rsa -in C:\https\ecmxtserver.agilent.com.key -out C:\https\ecmxtserver.agilent.com.unencrypted.key -passin pass:<password>`
- 5 Crie um arquivo de senha de chave. Por exemplo:
`echo|set /p="<password>" > c:\https\ecmxtserver.agilent.com.txt`

Solicitar o certificado e reconfigurar o proxy reverso

NOTA

Se a senha do OLSS padrão não foi alterada durante a instalação do sistema, ela deve ser alterada antes de executar o Utilitário de Configuração.

- 1 Acesse o seu provedor confiável de certificados com o arquivo .csr criado e solicite o certificado. O provedor pode ser a Infraestrutura de Chave Privada (PKI) em sua organização ou um fornecedor comercial, como a DigiCert.
 O seu provedor de certificados lhe enviará certificados no formato de .cer, .crt, .der, .pem, .p7b ou .pfx.
- 2 Inicie o Utilitário de Configuração no **Menu Iniciar do Windows > Agilent Technologies > Utilitário de Configuração** ou inicie a Etapa 4 do instalador do OpenLab Server/ECM XT Server.
- 3 Prossiga para a página Configuração de Certificado.
- 4 Selecione **Usar certificado personalizado existente** e, em seguida, selecione o formato do seu certificado e informações necessárias:

Formato do certificado CRT_NO_KEY: Seu provedor confiável de certificados entregará seu certificado do servidor no formato x509 DER (binário codificado) ou x509 PEM (BASE64 codificado). Os certificados podem ter as extensões de nome de arquivo .cer, .crt ou .der. Por exemplo, arquivo de certificado de servidor: C:\https\ecmxtserver.agilent.com.crt /.cer /.der.

- Insira ou pesquise para selecionar seu arquivo de Certificado. Por exemplo, C:\https\ecmxtserver.agilent.com.crt

- Insira ou pesquise para selecionar sua Chave Privada (descriptorgrada). Por exemplo, C:\https\ecmxtserver.agilent.com.unencrypted.key.
- Insira ou pesquise para selecionar o seu Caminho de Senha de Certificado. Por exemplo, C:\https\ecmxtserver.agilent.com.txt.

Formato de certificado PEM_NO_KEY: Seu provedor confiável de certificados entregará seu certificado do servidor no formato x509 PEM (BASE64 codificado). Os certificados têm a extensão de nome de arquivo .pem. Por exemplo, certificado do servidor: C:\https\ecmxtserver.agilent.com.pem.

- Abrir o certificado com o notepad mostra apenas que um certificado está presente, mas nenhuma chave privada.

Insira as informações necessárias para o formato do certificado:

- Insira ou pesquise para selecionar seu arquivo de Certificado. Por exemplo, C:\https\ecmxtserver.agilent.com.pem.
- Insira ou pesquise para selecionar sua Chave Privada (descriptorgrada). Por exemplo, C:\https\ecmxtserver.agilent.com.unencrypted.key.
- Insira ou pesquise para selecionar o seu Caminho de Senha de Certificado. Por exemplo, C:\https\ecmxtserver.agilent.com.txt.

Formato do certificado PEM_WITH_KEY: Seu provedor confiável de certificados entregará seu certificado do servidor no formato x509 PEM (BASE64 codificado). Os certificados têm a extensão de nome de arquivo .pem e incluem uma chave privada descriptorgrada. Por exemplo, certificado do servidor: C:\https\ecmxtserver.pem.

- Abrir o certificado com o notepad mostra que um certificado e uma chave privada descriptorgrada estão presentes.
- Se a chave privada no arquivo .pem estiver criptografada, consulte o formato de Certificado PEM_NO_KEY.

Insira as informações necessárias para o formato do certificado:

- Insira ou pesquise para selecionar seu arquivo de Certificado. Por exemplo, C:\https\ecmxtserver.agilent.com.pem.
- Insira ou pesquise para selecionar sua Chave Privada (descriptorgrada). Por exemplo, C:\https\ecmxtserver.agilent.com.pem.
- Insira ou pesquise para selecionar o seu Caminho de Senha de Certificado. Por exemplo, C:\https\ecmxtserver.agilent.com.txt.

Formato de certificado PFX: Seu provedor confiável de certificados entregará o certificado do servidor e a chave privada como parte de um contêiner de certificados pkcs nº 12 protegido por senha. Os certificados têm a extensão de nome de arquivo .pfx ou .p12 e incluem o certificado do servidor, bem como a cadeia do certificado até a autoridade do certificado raiz: Por exemplo, Contêiner de certificados: C:\https\ecmxtserver.agilent.com.pfx / .p12.

- Insira ou pesquise para selecionar seu arquivo de Certificado. Por exemplo, C:\https\ecmxtserver.agilent.com.pfx
- Insira ou pesquise para selecionar sua Chave Privada (descriptorgrada). Por exemplo, C:\https\ecmxtserver.agilent.com.pfx
- Insira ou pesquise para selecionar o seu Caminho de Senha de Certificado. Por exemplo, C:\https\ecmxtserver.agilent.com.txt

O arquivo .txt deve ser modificado para conter apenas a senha dentro, a qual é fornecida pela autoridade de certificado.

Formato do certificado P7B: Seu provedor confiável de certificados entregará o certificado do servidor como parte de um contêiner de certificados pkcs nº 7. Os certificados têm a extensão de nome de arquivo .p7b e incluem o certificado do servidor, bem como a cadeia do certificado até a autoridade do certificado raiz. Por exemplo, Contêiner de certificados:

C:\https\ecmxtserver.agilent.com.p7b.

- Insira ou pesquise para selecionar seu arquivo de Certificado. Por exemplo, C:\https\ecmxtserver.agilent.com.p7b
- Insira ou pesquise para selecionar sua Chave Privada (descriptografada). Por exemplo, C:\https\ecmxtserver.agilent.com.unencrypted.key.
- Insira ou pesquise para selecionar o seu Caminho de Senha de Certificado. Por exemplo, C:\https\ecmxtserver.agilent.com.txt.

- 5 Clique em **Próximo** para continuar com a reconfiguração do servidor.
- 6 Se solicitado, insira as credenciais de Administrador do OpenLab Shared Services (OLSS). (A senha-padrão do OLSS deve ter sido alterada antes de executar o Utilitário de Configuração.)
- 7 Após os serviços serem interrompidos e as alterações aplicadas, a configuração do certificado personalizado é aplicada ao proxy reverso.
- 8 Reconfigure as configurações do servidor e reative usando as etapas na seção a seguir.

Reconfigurar as configurações do servidor e reativar

- 1 No menu Iniciar do Windows, selecione **Agilent Technologies > Shared Services Maintenance** e selecione a guia **Configurações do Servidor**.
 - a Adicione o servidor.
 - b Insira um nome para o servidor.
Servidor: <Server-FQDN>
 - c Descrição: Opcional
 - d Defina o servidor adicionado como padrão.
- 2 Inicie o Control Panel para OpenLab.
 - a Administração > Licenças
 - b Altere o nome do servidor para <Server-FQDN>
- 3 Feche o Control Panel para OpenLab.
- 4 Reinicie o serviço OpenLab Shared Services.
- 5 No Control Panel para OpenLab, vá para **Administração > Configuração de Sistema > Editar Configurações do Sistema**.
 - a Na lista suspensa **Selecione outra opção da lista se desejar usar um tipo de armazenamento diferente**, selecione **Secure Storage**.
 - b Clique em **Próximo**.
 - c Selecione **Alterar o servidor**.
 - d Para o servidor do Secure Storage, insira o <Server-FQDN> e clique em **Ativar**.
 - e Clique em **Próximo**, em seguida, clique em **Aplicar** e confirme que deseja fazer as alterações.

- 6 Abra o editor de registro do Windows.
 - a Vá para Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Agilent\Services\ActivityLog.
 - b Altere o valor de "SharedServicesHost" de localhost para <Server-FQDN>.
- 7 Se não for prosseguir para as outras etapas, faça uma reinicialização.

NOTA

Para obter informações sobre portas abertas por produtos OpenLab, consulte o *Guia de Requisitos de Hardware e Software do OpenLab Server e ECM XT* fornecido com o software.

Desabilitar TLS/SSL

CUIDADO

TLS 1.0, TLS 1.1 e SSL 3.0 não são exigidos pelo OpenLab Server/ECM XT e representam um risco de segurança. Desative-os conforme as instruções da Microsoft.

NOTA

O TLS 1.2 (ou superior) suporta uma grande variedade de Cipher Suites, algumas das quais podem ser vulneráveis a ataques. O OpenLab Server/ECM XT suporta todas as Cipher Suites do TLS 1.2 (ou superior) e não é impactado se alguma Cipher Suite fraca ou vulnerável for desabilitada pelas suas políticas de TI.

Quando você desabilitar um protocolo de segurança, certifique-se de desabilitá-lo em todos os computadores do sistema (servidor de aplicativos, AICs e clientes CDS).

Cabeçalho do servidor

As varreduras de segurança podem reportar um aviso se a resposta HTTP de um servidor Web incluir informações sobre a tecnologia do servidor Web. Se você deseja não ter informações sobre a tecnologia do servidor Web, é necessário desativar a resposta HTTP no nível do sistema operacional.

Por padrão, o HTTP.SYS da Microsoft gera cabeçalhos de servidor. Os cabeçalhos de servidores são desativados no registro do Windows.

Para desativar o cabeçalho do servidor, abra o editor de registro do Windows, vá para

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\HTTP\Parameters\

crie um DWORD com o nome DisableServerHeader e defina o valor como 2.

Reiniciar o servidor

Quando terminar de fazer a segurança do sistema, reinicie o servidor.

Manutenção de Rotina do Servidor 33

Atualizar estatísticas do banco de dados 33

Procedimentos de Manutenção do banco de dados PostgreSQL 33

Procedimentos de Manutenção do SQL Server 35

Monitorar utilização de recursos no servidor OpenLab Server/ECM XT 36

Melhores práticas adicionais 36

Domínio do Windows 37

Atualizar o Domínio, Nome de Usuário ou Senha de seu servidor 37

Ativar permissão de leitura para um usuário 37

Configurações do servidor 38

Arquivar 39

Etapa 1: Adicionar um local de armazenamento de acervo ao Secure Storage 39

Etapa 2: Configurar um agendamento para bloquear as pastas automaticamente 39

Etapa 3: Realocar pastas para o local de armazenamento de acervo 40

Exemplo: Configurar armazenamento automático de acervo de arquivos 40

O programa utilitário **OpenLab Shared Services Maintenance** é automaticamente instalado com o software OpenLab para ajudar os administradores a gerenciar o sistema.

Para abrir o programa, selecione **Iniciar Windows > Agilent Technologies > Shared Services Maintenance**.

O usuário deve ter privilégios de administrador do Windows para acessar este programa.

CUIDADO

Após a instalação, não altere o nome do host do servidor. Entre em contato com o Suporte da Agilent para alteração do nome do host.

Manutenção de Rotina do Servidor

Atualizar estatísticas do banco de dados

Para manter o desempenho ideal do banco de dados, atualize periodicamente as estatísticas do banco de dados do servidor OpenLab Server/ECM XT. Estas estatísticas são utilizadas pelo mecanismo do banco de dados para determinar a forma ideal para executar as consultas.

Atualize as estatísticas dos bancos de dados do servidor OpenLab Server/ECM XT e do OpenLab Shared Services. Se tiverem sido escolhidos nomes de bancos de dados personalizados durante a instalação, utilize os nomes corretos das suas notas de instalação.

Procedimentos de Manutenção do banco de dados PostgreSQL

Para o banco de dados PostgreSQL, estes procedimentos devem ser executados regularmente. A frequência depende da utilização do sistema. Como orientação, é necessário realizar estes procedimentos pelo menos todas as vezes que um backup completo é realizado.

Executar a ferramenta de gerenciamento de dados PostgreSQL

- 1 Vá para **Menu Iniciar do Windows > pgAdmin 4 > pgAdmin4 v6**. Se você estiver executando o pgAdmin pela primeira vez, defina a senha mestra e adicione um servidor ao grupo de servidores. Clique com o botão direito em **Servidores** e selecione **Registrar > Servidor** para adicionar um servidor.
- 2 Na guia **Geral**, insira *localhost* no campo **Nome**.
- 3 Na guia **Conexão**, insira *localhost* como o **Nome/endereço do host** e insira a senha do usuário postgres. A senha foi configurada durante a instalação. Selecione **Salvar senha?** para salvar a senha.
- 4 Clique em **Salvar**. *localhost* agora é exibido no grupo **Servidores**.
- 5 Expanda *localhost* e, em seguida, expanda o **Bancos de dados**.
- 6 Clique duas vezes em **OLSharedServices** e **datarepo** para conectar os dois bancos de dados.

Atualizar estatísticas utilizando o Assistente de Manutenção

- 1 Inicie o **PostgreSQL pgAdmin**, conecte-se como administrador do banco de dados e selecione o banco de dados para o qual deseja atualizar as estatísticas. O nome de usuário padrão do administrador do banco de dados é "postgres" e a senha padrão é a senha definida na **Etapa 1 – Instalar ou Atualizar os Pré-requisitos do Software** do processo de instalação do OpenLab Server/ECM XT.
- 2 Clique com o botão direito no banco de dados e selecione **Manutenção**. O seguinte formulário é exibido.

- 3 Escolha **ANALISAR** e clique em **OK** para analisar o banco de dados.

Manutenção adicional para o banco de dados PostgreSQL

O PostgreSQL é compatível com alguns comandos de manutenção adicionais que podem ser úteis para manter o sistema do banco de dados funcionando perfeitamente. Isto inclui VACUUM e REINDEX. Consulte a documentação do PostgreSQL para obter mais detalhes sobre estes comandos.

NOTA

É possível agendar tarefas de manutenção usando o pgAgent.

CUIDADO

Aplique apenas **Service Packs** ou **Hotfixes** fornecidos pela Agilent no seu servidor PostgreSQL OpenLab.

Procedimentos de Manutenção do SQL Server

Verifique se há pelo menos 4 GB reservados para o sistema operacional Windows.

Ajuste de desempenho do Microsoft SQL Server

Se o número de documentos atingir mais de 10 milhões, o OpenLab Server/ECM XT com SQL Server poderá ficar lento nas seguintes áreas devido à definição da detecção de parâmetros do SQL Server como Ligada:

- 1 Tempo de inicialização
- 2 Lista inicial de arquivos na Web e DA após a reinicialização do servidor

Caso alguma das situações acima ocorra, não defina a detecção de parâmetros como Desligada, pois isso não é suportado.

Índices de cobertura inadequados muitas vezes podem ser a principal causa de detecção de parâmetros. O SQL Server poderá escolher um plano de Pesquisa de Chave para um pequeno número de valores. Um índice em cluster procura ou verifica um grande número de valores. Com um índice de cobertura, o otimizador não fará essas escolhas e, geralmente, você terá um plano de execução mais estável.

- 3 Recrie índices com base nas seguintes recomendações. Execute uma verificação de fragmentação do índice e:
 - Recompile tudo que estiver >30% fragmentado.
 - Reorganize tudo que estiver entre 5 e 30% fragmentado. Consulte <https://docs.microsoft.com/en-us/sql/relational-databases/indexes/reorganize-and-rebuild-indexes> para obter mais informações.

Otimizar o Microsoft SQL Server para funcionar com o Secure Storage

Para garantir que o seu desempenho não se degrade, realize as seguintes operações de manutenção semanais no seu SQL Server.

- Recalcule as estatísticas ao executar o comando: `EXEC sp_updatestats`
- Limpe os buffers ao executar o comando: `DBCC DROPCLEANBUFFERS`
- Limpe o cache ao executar o comando: `DBCC FREEPROCCACHE`

Atualizar estatísticas utilizando o Assistente do Plano de Manutenção

Para o banco de dados do Microsoft SQL Server, o procedimento para atualizar estatísticas pode ser facilmente automatizado utilizando o SQL Server Management Studio.

- 1 Inicie o **SQL Server Management Studio** e conecte-se como administrador do banco de dados.
- 2 Expanda o servidor.
- 3 Expanda a pasta de gerenciamento.
- 4 Clique com o botão direito em **Planos de manutenção** e selecione **Assistente de plano de manutenção**. Utilize o assistente para criar um plano personalizado para atender às suas necessidades de manutenção.
 - a Selecione uma **Programação semanal** para ser executada em um momento em que possa haver atividade mínima (por exemplo, domingo 12:00).
 - b Selecione **Atualizar estatísticas** como a tarefa de manutenção.

- c Escolha o banco de dados do servidor OpenLab Server/ECM XT (datarepo) e o banco de dados do Shared Services (OLSharedServices) como o banco de dados relativo ao qual a tarefa será executada.

Mover seu servidor

Para mover seu servidor de um domínio para um grupo de trabalho ou de um domínio para outro domínio, o SQL Server deve ser configurado com uma conta local (não uma conta de domínio). Entre em contato com o Suporte da Agilent para ajuda ao mover seu servidor.

Monitorar utilização de recursos no servidor OpenLab Server/ECM XT

Os arquivos de dados, índices e o banco de dados são armazenados no disco rígido do servidor ou no AWS S3. Dependendo da configuração do seu servidor, pode haver uma ou mais unidades de disco.

Os administradores do sistema devem monitorar regularmente o uso do espaço em disco em todos os discos onde os dados são armazenados. Quando os discos se aproximam de 80% da capacidade, considere aumentar o espaço em disco. O uso da CPU, da memória e da rede deverá ser monitorado para verificar os gargalos no desempenho do servidor.

Melhores práticas recomendadas para monitoramento do uso de recursos

- 1 Monitore o uso do disco do servidor OpenLab Server/ECM XT no mínimo uma vez por semana.
- 2 Opcionalmente, implemente ferramentas de monitoramento automático de espaço em disco que enviem e-mails de alerta quando o uso do disco exceder os thresholds. Os exemplos de tais ferramentas são: Monit, Munin, Cacti e Nagios.
- 3 Monitorar o uso dos recursos do sistema, tais como memória, CPU e taxa de transferência de rede. O monitor de desempenho do Windows pode ser utilizado com esse propósito.

Melhores práticas adicionais

- Aplicar atualizações e patches de terceiros no servidor OpenLab Server/ECM XT.
- Aplicar atualizações do software Agilent.

Aplicar atualizações de software do Secure Storage e do Shared Services em seu servidor OpenLab Server/ECM XT. Ao receber uma notificação de atualização, tome nota e leia as informações para determinar se a atualização é aplicável e a sua urgência.

Domínio do Windows

Atualizar o Domínio, Nome de Usuário ou Senha de seu servidor

Se for usada a autenticação por domínio do Windows para identificar os usuários do OpenLab, este deve ter acesso ao servidor onde estas credenciais se encontram armazenadas.

Utilize **Domínio do Windows** para especificar ou alterar as credenciais que o OpenLab utilizará para acessar o servidor do seu domínio do Windows. Este recurso só pode acessar as credenciais armazenadas no computador no qual você abriu o programa utilitário Shared Services Maintenance.

Para especificar ou alterar o **Domínio**, **Nome do usuário** ou **Senha** para a conta do Windows que será usada para acessar o servidor do domínio do Windows, use o programa **utilitário Shared Services Maintenance** que está instalado no servidor.

Ativar permissão de leitura para um usuário

Ao utilizar a autenticação de domínio do Windows, o OpenLab Server/ECM XT lê os atributos de usuário para obter informações se os usuários devem ou não alterar sua senha do OpenLab. Se a permissão de leitura não tiver sido concedida ao usuário, o OpenLab Server/ECM XT presume que a senha do usuário expirou e nega o acesso.

Para ativar permissão de leitura para um usuário:

- 1 Em um controlador de domínio, abra **Usuários e Computadores do Active Directory**.
- 2 Selecione **Ver > Recursos Avançados**.
- 3 Em **Usuários**, clique com o botão direito e selecione **Propriedades**.
- 4 Na guia **Segurança**, selecione **Autenticação de Usuários**.
- 5 Selecione a permissão **Leitura** e clique em **OK**.

Configurações do servidor

Em uma configuração cliente-servidor, utilize as **Configurações do Servidor** para gerenciar as conexões do servidor para o seu sistema local. A lista de servidores exibida determina a quais servidores os usuários podem se conectar ao iniciar sessão no OpenLab. Administradores podem impedir que usuários escolham um servidor não-padrão dessa guia.

Este recurso gerencia conexões do servidor para o computador no qual você está usando o programa **utilitário Shared Services Maintenance**.

As conexões do servidor para os clientes em um sistema cliente/servidor são gerenciadas por meio de cada cliente. Portanto, para alterar as conexões do servidor para um cliente, acesse o programa **utilitário Shared Services Maintenance** instalado nesse cliente.

Arquivar

O arquivamento de conteúdo é importante para a manutenção do seu sistema e deve ser realizado com regularidade.

O procedimento a seguir descreve como arquivar arquivos automaticamente usando a Administração de Armazenamento. Você deve ter os privilégios para *Gerenciar armazenamento de arquivos*, *Gerenciar locais de armazenamento* e *Agendar bloqueio de arquivo* para concluir este procedimento. Os procedimentos são realizados em pastas dentro do armazenamento de conteúdo seguro. Todos os arquivos e subpastas dentro de uma pasta são bloqueados e, em seguida, realocados para um local de armazenamento de acervo. Não é possível bloquear e arquivar automaticamente um único arquivo. No entanto, é possível bloquear e desbloquear arquivos ou pastas individuais do Navegador de Conteúdo.

NOTA

É possível inverter a ordem das Etapas 2 e 3.

Etapa 1: Adicionar um local de armazenamento de acervo ao Secure Storage

Na guia Gerenciar Armazenamento da Administração de Armazenamento, adicione um local de armazenamento de acervo. Para o procedimento para adicionar um local de armazenamento, consulte o tópico *Adicionar um local de armazenamento* na Ajuda online da Administração de Armazenamento. Este será o seu local de armazenamento de acervo. Os locais de armazenamento podem ser locais, em rede ou um local AWS S3. Crie quantos locais de armazenamento desejar, mas só é possível designar um local de armazenamento principal. O local de armazenamento principal é onde os arquivos são armazenados por padrão, não o utilize para armazenamento de acervo.

Etapa 2: Configurar um agendamento para bloquear as pastas automaticamente

Antes de realocar as pastas para o local de armazenamento de acervo, bloqueie-as para evitar futuras alterações. A função Agendar Bloqueio na Administração de Armazenamento permite bloquear pastas automaticamente com um agendamento baseado em critérios selecionados. Para obter informações sobre como configurar um agendamento de bloqueio, consulte o tópico *Configurar um agendamento de bloqueio automático* na Ajuda online da Administração de Armazenamento.

Etapa 3: Realocar pastas para o local de armazenamento de acervo

Usando o procedimento descrito no tópico *Configurar realocação* na Ajuda online da Administração de Armazenamento, crie uma tarefa de realocação ou configure um agendamento de realocação para a realocação das pastas que você deseja arquivar no local de armazenamento de acervo. As tarefas de realocação podem ser configuradas para serem executadas imediatamente ou automatizadas para serem executadas em um agendamento. Realocar arquivos para um local de armazenamento de acervo libera espaço no seu local de armazenamento principal e ajuda a manter o seu sistema com o máximo desempenho.

NOTA

A realocação move o conteúdo da pasta para um local de armazenamento diferente. Ela não modifica a estrutura da pasta de conteúdo no Navegador de Conteúdo.

Exemplo: Configurar armazenamento automático de acervo de arquivos

Neste exemplo, configure um armazenamento automático de acervo de arquivos em uma pasta nomeada Test1030 com uma data de modificação do conteúdo superior a 1 mês.

- 1 Na guia **Gerenciar Armazenamento**, crie um novo local de armazenamento:
C:\SSStorage\Archive1. É para onde as pastas serão realocadas para armazenamento de acervo.
- 2 Em **Agendar Bloqueio > Configurar Agendamento de Bloqueio**, selecione a pasta Test1030 e crie um agendamento de bloqueio automático para bloquear todos os arquivos na pasta que tem uma **Data de Modificação do Conteúdo** superior a um mês. O agendamento está configurado para ser executado todo primeiro domingo à 00:00. Salve o agendamento de bloqueio. O agendamento salvo pode ser visualizado, excluído ou modificado em **Agendar Bloqueio > Agendamentos de Bloqueio**.
- 3 Em **Realocar Arquivos > Configurar Realocação**, selecione a pasta Test1030 para realocação e crie um agendamento para realocar os arquivos que têm uma **Data de Modificação do Conteúdo** superior a um mês. A realocação está agendada para ser executada todo primeiro domingo do mês à 01:00. Salve o agendamento da realocação. O agendamento salvo pode ser visualizado, excluído ou modificado em **Realocar Arquivos > Agendamentos de Realocação**.

Informações Importantes sobre Backup e Restauração	42
Usando o Amazon Web Services S3 como um local de backup	43
Criar um Plano de Recuperação de Desastres	44
Usar os Utilitários de Backup e Restauração	46
Backup do OpenLab Server/ECM XT Usando o Utilitário de Backup	47
Procedimentos para uso do Utilitário de Backup	49
Verificação do backup	52
Backup incremental de bancos de dados PostgreSQL	54
Configurar backup incremental usando a Ferramenta de Configuração Incremental	55
Configurar o diretório de dados personalizado do banco de dados PostgreSQL	56
Restaurar o OpenLab Server/ECM XT Usando o Utilitário de Restauração	57
Restaurar um sistema com banco de dados PostgreSQL ou Microsoft SQL	58
Reconfiguração durante a restauração	60

Informações Importantes sobre Backup e Restauração

O backup periódico de cada servidor OpenLab Server/ECM XT é obrigatório. Os administradores do servidor OpenLab Server/ECM XT criam backups completos periódicos e backups diferenciais entre os backups completos. Esses backups são a única forma de restaurar um servidor OpenLab Server/ECM XT caso ocorra uma falha de hardware ou software.

O backup apenas reduz a quantidade de perda de dados caso ocorra uma falha de sistema catastrófica. A realização de backups garante que todos os dados confirmados no momento do backup podem ser restaurados. Os dados colocados em espera para carregar e que ainda não foram confirmados, adicionados ou atualizados no sistema após a realização do backup não serão recuperáveis por meio de restauro de um backup.

Também é obrigatório testar os procedimentos de restauração para garantir que os backups sejam realizados de forma apropriada e que possam ser usados para uma restauração. Para uma restauração eficaz, deve ser criado um plano de recuperação de desastres. Consulte **"Criar um Plano de Recuperação de Desastres"** na página 44.

O OpenLab Server/ECM XT armazena arquivos e índices no sistema de arquivos do seu servidor. O local dessa pasta é determinado quando o produto é instalado. Outros dados, como informações da pasta, registros de auditoria e assinaturas, são armazenados em um banco de dados relacional.

Um backup completo captura um conjunto completo de dados do OpenLab Server/ECM XT, incluindo arquivos carregados e seus bancos de dados. Um backup incremental contém alterações que ocorreram desde o último backup completo. O processo do backup incremental é mais rápido que o do backup completo, uma vez que apenas os elementos modificados são incluídos no backup.

NOTA

Em uma configuração típica, a ferramenta Backup e Restauração pode fazer backup de cerca de 150 a 200 GB/h (com cerca de 50.000 arquivos) em um compartilhamento de rede conectado através de uma rede local de, pelo menos, 1 GB/s. A Verificação de Arquivos pode verificar cerca de 600 arquivos por minuto. Em um cenário de restauração, considere o tempo necessário para a verificação do arquivo. Esses valores podem variar, dependendo da configuração do hardware e do tamanho médio do arquivo.

NOTA

A ferramenta Backup e Restauração 1.0 para o OpenLab CDS e o OpenLab Server/ECM XT versão 2.8 não pode restaurar os backups criados com as versões anteriores do OpenLab CDS e do OpenLab Server/ECM XT. Para restaurar um backup do OpenLab CDS 2.7, use a ferramenta Backup e Restauração da mídia de instalação do OpenLab 2.7.

Usando o Amazon Web Services S3 como um local de backup

- Assegure-se de que o bucket do S3 não seja "publicamente" acessível pela internet. Use controles centralizados para limitar o acesso.
- Siga os princípios de "acesso menos privilegiado". Conceda apenas as permissões necessárias para executar a tarefa
- Se você planeja usar o S3 como local de backup para seu sistema usando as ferramentas Backup/Restauração do OpenLab, atribua as seguintes permissões (além das permissões definidas acima) ao bucket que conterá os backups.

s3:DeleteObjectVersion

s3:GetObjectVersionTagging

s3:ListBucketVersions

s3:PutObjectVersionTagging

s3:DeleteObjectVersionTagging

- Habilite a criptografia do lado do Servidor.
- Habilite o controle de versão de objetos.

Criar um Plano de Recuperação de Desastres

Prepare um plano de recuperação para o caso improvável de o OpenLab Server/ECM XT ficar inoperável devido a uma falha de hardware ou software. Esse plano deve incluir informações e procedimentos para restaurar completamente o sistema operacional, o software OpenLab Server/ECM XT e os dados, se necessário, em um servidor físico diferente. Certifique-se de que o plano de recuperação de desastres tenha sido testado e cujo funcionamento tenha sido confirmado.

Ao desenvolver o seu plano de recuperação de desastres, considere o seguinte:

- Determine a frequência dos backups necessários. Por exemplo, qual é o número máximo aceitável de amostras perdidas em caso de falha (amostras que exigiriam repetição)? Geralmente, há um equilíbrio entre a frequência dos backups e o custo/esforço de restauração, especialmente para sistemas grandes.
- Qual é o melhor método de backup/restauração, com base na topologia do sistema e nos requisitos de disponibilidade?
 - Utilitário de Backup/Restauração (disponível apenas para topologia tudo-em-um). Os utilitários fornecem backups diários completos ou incrementais.
 - Procedimentos manuais personalizados (recomendados para sistemas maiores). Esses procedimentos consistem em um cold backup inicial da configuração do sistema, dos bancos de dados e do armazenamento do conteúdo. Seguidos da realização regular de:
 - Cold backups de bancos de dados, arquivos e configuração.
 - Hot backups automatizados de bancos de dados e backup incremental de arquivo
 - Registro contínuo da transação do banco de dados com backup contínuo de arquivos em combinação com backups completos regulares

NOTA

A ordem das opções representa a crescente complexidade e o esforço de implantação.

O backup e a restauração do OpenLab Server/ECM XT são suportados apenas para exatamente o mesmo tipo de configuração de banco de dados. Se você tentar o backup e a restauração entre diferentes tipos de bancos de dados arquivados (incluindo os mesmos bancos de dados com configurações diferentes), o Control Panel exibirá um erro. O "Plano de recuperação de desastres" deve incluir o seguinte:

- Informações sobre o hardware do servidor: informações de configuração de CPU, memória e disco rígido
- Identidade do servidor: Nome, IP, domínio, URL etc.
 - Informações sobre o administrador do servidor: nome de usuário e senhas para iniciar sessão no servidor. Se aplicável, nomes de usuários e senhas para o banco de dados.
 - É necessário que todos os nomes de usuário e senhas do banco de dados no Sistema-alvo (onde você deseja restaurar o backup) sejam os mesmos do Sistema de origem (de onde você fez o backup).
- Informações sobre o software do servidor: versão do SO, nível de correções
- Parâmetros de instalação do OpenLab Server/ECM XT. É necessário que o sistema de restauração tenha o mesmo caminho de instalação do OpenLab Server/ECM XT que o sistema onde o backup foi criado.
 - Pasta de instalação
 - Arquivo de registro da instalação

Procedimentos de Backup e Restauração

Criar um Plano de Recuperação de Desastres

- Tipo de banco de dados do OpenLab Server/ECM XT
- Conteúdo do OpenLab Server/ECM XT
- Nome do banco de dados do conteúdo seguro do OpenLab Server/ECM XT
- Idioma do Shared Services
- Nome do banco de dados Shared Services
- Licenças instaladas
- Aplicações registradas
- Informações sobre software de terceiros: aplicativos e suas revisões e caminhos de instalação
- Procedimentos para sua topologia. Consulte "**Usar os Utilitários de Backup e Restauração**" na página 46 ou **Capítulo 6**, "Procedimentos Manuais de Cold Backup e Restauração".
- Local da mídia de backup e detalhes da organização
- O servidor de banco de dados remoto está configurado corretamente. Consulte "Configurar um Servidor de Banco de Dados Remoto" na *Guia de Instalação do OpenLab Server/ECM XT*.

Usar os Utilitários de Backup e Restauração

Os Utilitários de Backup e Restauração são ferramentas que facilitam o backup e a restauração de seu sistema OpenLab Server/ECM XT.

Para uma topologia tudo-em-um, você pode usar as ferramentas automatizadas para backup e restauração descritas nas seções a seguir. Para topologia empresarial, use os procedimentos manuais de backup e restauração descritos em **Capítulo 6**, "Procedimentos Manuais de Cold Backup e Restauração". A tabela seguinte descreve as topologias do OpenLab Server/ECM XT suportadas pelos Utilitários de Backup e Restauração.

CUIDADO

A varredura antivírus durante o backup pode impedir a conclusão com sucesso do backup. Certifique-se de que a localização do backup seja excluída para varreduras regulares/agendadas e proteção em tempo real. Se não for possível excluir a localização do backup da proteção em tempo real e não for possível desativar a proteção em tempo real, é possível que as tarefas de backup finais não sejam concluídas com sucesso.

Para ajudar a evitar essas falhas, há uma configuração de Atraso e Repetição. Por padrão, isto é definido para 3 tentativas com 10 segundos de atraso. É possível modificar essa configuração na seção Backup > BackupFinalizationSettings do arquivo configuration.xml localizado na pasta %ProgramData%\Agilent\Installation. Os privilégios de Administrador do Sistema são necessários para atualizar este arquivo. Os valores aceitáveis são Atraso maior que 0 e Repetição maior que 1. Aplica-se Atraso e Repetição ao "Fazer backup agora" na página Processamento antes da primeira etapa e quando um backup é iniciado a partir de um "Backup por agendamento".

Se algum antivírus estiver sendo executado durante o backup, verifique se o backup foi concluído com sucesso seguindo estas etapas:

Após a conclusão do backup, verifique se a localização do backup contém apenas a(s) subpasta(s) "Atual" (ou "Atual" e "Incremental")

Verifique se o arquivo de registro correspondente ao horário do backup contém uma entrada informando "O backup foi concluído" no final. Os logs de backup são colocados na pasta "C:\ProgramData\Agilent\LogFiles\Backup".

Tabela 5. Topologias com suporte para Utilitários de Backup e Restauração

Topologia	Utilitário de Backup	Utilitário de Restauração	Observações
All-in-One	+	+	Procedimentos manuais também disponíveis.
2-3-Servidores	Apenas manual	Apenas manual	Use procedimentos manuais.

Backup do OpenLab Server/ECM XT Usando o Utilitário de Backup

Use o Utilitário de Backup para fazer backups imediatos ou agendados para topologias com suporte. O Utilitário de Backup é compatível com backups completos e incrementais. Para obter uma lista das topologias suportadas pelo Utilitário de Backup, consulte **"Usar os Utilitários de Backup e Restauração"** na página 46.

O backup captura um conjunto completo de dados do OpenLab, incluindo:

- Arquivos de configuração
- Bancos de dados para Shared Services e Data Repository
- Locais de armazenamento local
- Serviço de certificados
- Serviço Rabbit MQ
- Serviço Reverse Proxy

NOTA

O Utilitário de Backup faz backup apenas dos dados do OpenLab. O cliente é responsável por fazer backup dos elementos principais do banco de dados, como Master e MSDB, como parte da manutenção geral do banco de dados.

NOTA

O Utilitário de Backup não faz backup de dados de um local de armazenamento do AWS S3.

NOTA

O Utilitário de Backup não faz backup de certificados personalizados usados para conexão segura. Se forem usados certificados personalizados, faça backup deles manualmente e mantenha-os em um local seguro para uso durante o processo de restauração.

NOTA

O usuário deverá ter as permissões "Logon como uma tarefa em lote" e "Logon como um serviço" e ser um administrador no ECM XT Server e no servidor de banco de dados caso o sistema esteja configurado com uma conta de usuário especificada (não do sistema).

CUIDADO

Se você usar o Utilitário de Backup do Agilent OpenLab para agendar backups, não use o SQL Server Management Studio, o SQL Scripts ou ferramentas para fazer backup dos bancos de dados do OpenLab. Isso impedirá que a ferramenta execute backups incrementais.

Espaço necessário

O espaço livre necessário para o procedimento de backup depende de diferentes fatores, incluindo a configuração do servidor, a localização do backup e o tamanho do backup do banco de dados. No caso de uso intensivo de recursos, certifique-se de que o espaço livre na localização do backup seja, pelo menos, duas vezes superior à soma do tamanho de todo o armazenamento de arquivos no local e do banco de dados. Isso é necessário para impedir que um backup anteriormente realizado com sucesso seja reescrito por um backup que, por algum motivo, não foi concluído.

Os Utilitários de Backup e Restauração usam pastas de banco de dados definidas como locais de backup temporários durante o backup/restauração de/para o local de backup do AWS S3:

- Diretório de dados para o banco de dados PostgreSQL. Consulte "[Configurar o diretório de dados personalizado do banco de dados PostgreSQL](#)" na página 56.
- Local de backup padrão para o banco de dados MS SQL. Siga o guia MS SQL para configurar o local de backup padrão. Certifique-se de que o novo local tenha permissões para credenciais de acesso e MSSQLSERVER (NT Service\MSSQLSERVER).

Verifique se o espaço no local definido seja suficiente para armazenar temporariamente o backup do banco de dados.

Configurar bancos de dados para backup incremental

Se você planeja usar backups incrementais, deve primeiro configurar os bancos de dados OLSS e PostgreSQL do Data Repository (se necessário). Consulte "[Backup incremental de bancos de dados PostgreSQL](#)" na página 54.

Solução de problemas

O Utilitário de Backup coleta logs na pasta %ProgramData%\Agilent\LogFiles\Backup. Durante o procedimento de backup, todas as etapas são verificadas e o procedimento será interrompido na primeira etapa falhada. Um link com a etapa falhada abre o arquivo de registro de backup atual para ajudar a identificar o problema. Em caso de falha no backup, o backup parcial será armazenado em uma pasta Temp na localização do backup.

Procedimentos para uso do Utilitário de Backup

Backup usando o Utilitário de Backup

Etapas	Opções	Observações
<p>1 Inicie o Utilitário de Backup em Iniciar > Agilent Technologies > Utilitário de Backup.</p> <p>Se for exibida uma solicitação de acesso ao Controle de Conta de Usuário, clique em Sim.</p> <p>Clique em Próximo.</p>	<p>A página Status exibe a data e a hora do último backup realizado com sucesso.</p> <p>Clique no link para acessar a localização do backup.</p>	<ul style="list-style-type: none"> São necessários privilégios de administrador do sistema para executar o Utilitário de Backup Se um backup estiver agendado, a página exibirá o status do backup atual e a data e hora iniciais do próximo backup. Se um backup estiver sendo feito, o status exibirá Em execução. Em caso de falha do backup agendado, o status exibe Falhou. O Último backup bem-sucedido mostra a data/hora em que o último backup bem-sucedido (tipos "por agendamento" ou "fazer backup agora") foi realizado e a respectiva localização. O link indica a localização do backup (local ou AWS S3); ele incluirá as informações logo após o primeiro backup realizado com sucesso. Reinicie o sistema se o fuso horário tiver sido alterado. Caso contrário, a data/hora na página Status poderá mostrar valores incompatíveis.
<p>2 Na página Opção de backup, selecione a opção de backup.</p>	<ul style="list-style-type: none"> Definir o agendamento de backup 	<ul style="list-style-type: none"> Use esta opção como parte de um procedimento de backup automático. Forneça o tipo de backup e as configurações de agendamento. O horário de agendamento usa um formato de 24 horas. É recomendável o agendamento de backups automáticos. Para desabilitar os backups automáticos durante períodos de manutenção, desmarque a caixa de seleção Habilitar agendamento de backup. Certifique-se de habilitar os backups agendados após a conclusão da manutenção.
	<ul style="list-style-type: none"> Fazer backup agora <ul style="list-style-type: none"> Hot backup Cold backup 	<ul style="list-style-type: none"> O backup usando o hot backup ou o cold backup começa imediatamente. Não tem impacto em um backup agendado. Esta opção pode ser útil para verificar a exatidão das configurações de backup, bem como o espaço em disco e o tempo necessários para um único backup. Além disso, essa opção pode fazer parte do teste de todo o procedimento de recuperação.

Procedimentos de Backup e Restauração

Procedimentos para uso do Utilitário de Backup

Backup usando o Utilitário de Backup (continuação)

Etapas	Opções	Observações
3 Na página Configurar, configure suas configurações de backup.	<ul style="list-style-type: none"> Para agendamento de backup, habilite e configure o agendamento de backups Selecione se pretende que o seu sistema esteja disponível durante o backup <ul style="list-style-type: none"> Sim para hot backup Não para cold backup Selecione para habilitar backups incrementais. Insira a hora e os dias para backups incrementais 	<ul style="list-style-type: none"> É altamente recomendável habilitar o backup por agendamento. Desmarcar a caixa de seleção Habilitar agendamento de backup desativa o backup agendado. Se backups completos e incrementais estiverem agendados para o mesmo dia, o backup completo será o executado. Os backups incrementais exigem que primeiro a opção de backup incremental seja configurada (consulte "Backup incremental de bancos de dados PostgreSQL" na página 54) e que então um backup completo seja realizado após a configuração bem-sucedida. (Se o MSSQL for usado como banco de dados, o backup incremental não exigirá configuração adicional.) Se um backup completo agendado falhar, os backups incrementais subsequentes falharão até o próximo backup completo agendado realizado com sucesso. Para evitar uma falha nos backups incrementais, execute um backup imediato no local designado para os backups agendados. Durante a configuração do backup incremental com o MSSQL, se um backup completo imediato estiver presente no local do backup, será exibido um aviso de backup incompatível. Para evitar uma falha nos backups incrementais, execute um backup completo imediato após enviar o backup agendado. Caso contrário, execute um backup agendado completo neste local ou use outro local onde o backup seja compatível.
	<ul style="list-style-type: none"> Para Backup agora, selecione se pretende que o seu sistema esteja disponível durante o backup <ul style="list-style-type: none"> Sim para hot backup Não para cold backup 	<ul style="list-style-type: none"> Hot backup: o sistema permanece operacional durante o backup Cold backup: requer a interrupção de todas as operações do OpenLab Server/ECM XT. O Utilitário de Backup realiza automaticamente essa ação.
4 Fornecer localização do backup		O backup pode ser configurado para uma pasta sem permissões para o usuário atual do Windows. O backup é executado a partir do usuário do sistema, o que permite salvar um backup bem-sucedido. Neste caso de backup agendado, o backup será executado, mas o usuário atual do Windows não poderá ver os resultados sem os privilégios apropriados.

Procedimentos de Backup e Restauração

Procedimentos para uso do Utilitário de Backup

Backup usando o Utilitário de Backup (continuação)

Etapas	Opções	Observações
	<ul style="list-style-type: none"> Sistema de arquivo 	<ul style="list-style-type: none"> A localização do backup destina-se a backup on-prem, local ou em um compartilhamento do Windows. A unidade de rede não é suportada. Se você estiver usando um compartilhamento de rede, o servidor deverá ser configurado com uma conta de usuário especificada. Para configurar o Servidor com esta configuração, execute Utilitário de Configuração do Servidor > Credenciais de Acesso. O usuário deve ter permissões de Logon como uma tarefa em lote e ser um administrador. A configuração do servidor com conta do SISTEMA suporta apenas pastas locais.
	<ul style="list-style-type: none"> AWS S3 (local do Amazon AWS S3) <ul style="list-style-type: none"> Fornecer chaves de acesso, nome e área de armazenamento da S3 	<ul style="list-style-type: none"> Habilite o versionamento de objetos na configuração de armazenamento do AWS S3. Certifique-se de que as configurações do AWS S3 sejam válidas. Uma mensagem será exibida no AWS S3 se o serviço estiver inacessível ou as configurações forem inválidas.
5 Fornecer credenciais do Shared Services	<ul style="list-style-type: none"> Validar credenciais da conta OLSS 	<ul style="list-style-type: none"> Insira credenciais válidas da conta OLSS. Não será possível continuar se por algum motivo a conta de usuário OLSS não conseguir fazer login (por exemplo, o usuário está temporariamente bloqueado ou o usuário está desativado). As contas de usuário OLSS para os processos de backup e restauração devem ter a função "Tudo" atribuída.
6 Configure as notificações. Se você tiver selecionado Backup agora, isso será ignorado.	<ul style="list-style-type: none"> Habilitar notificações de backup Endereço De Endereço Para 	<ul style="list-style-type: none"> Use um endereço "De" configurado no Control Panel. Para obter informações sobre como configurar os endereços de e-mail, consulte a ajuda online do Control Panel. Use uma vírgula para separar vários endereços "Para". Todos os endereços podem ser representados em formato longo (nome e e-mail) ou em formato abreviado (apenas e-mail).
	<ul style="list-style-type: none"> O Assunto começa com texto 	Isso especifica um prefixo no assunto do e-mail de notificação.
	<ul style="list-style-type: none"> Enviar uma mensagem de teste 	Use Enviar mensagem de teste para assegurar que as configurações de notificação estão corretas.
7 Revise e inicie o backup. Para iniciar o backup, clique em Aplicar .		<ul style="list-style-type: none"> É possível acompanhar o progresso na página Processamento. Após a conclusão da verificação, é fornecido um link para o relatório de verificação.

Backup usando o Utilitário de Backup (continuação)

Etapas	Opções	Observações
8	Assim que o backup for concluído, clique em Concluído .	

NOTA

Se você estiver usando o Sample Scheduler, deverá reiniciar os serviços do Sample Scheduler após um cold backup.

As pastas de backup são criadas na localização especificada ao executar o Utilitário de Backup.

Em caso de falha no backup, o backup parcial será salvo em uma pasta Temp na localização do backup.

NOTA

Em alguns casos, a verificação antivírus pode impedir a etapa final de renomear a pasta Temp para Atual. Nesse caso, a criação do arquivo backup.xml foi bem-sucedida, embora o backup tenha "falhado". Se esse foi o motivo da falha, é possível renomear manualmente a pasta Temp para Atual (se o backup completo foi realizado). Se o backup incremental foi executado, renomeie a pasta Temp para Incremental.

NOTA

Os backups podem levar muito tempo. Isto pode fazer com que o próximo backup agendado seja ignorado até que o backup anterior seja concluído. O próximo backup prosseguirá de acordo com o agendamento configurado. Consulte os registros de backup para obter o status e o horário, e reajuste o agendamento, se necessário.

CUIDADO

É possível alterar as configurações dos locais de armazenamento, como endereço ou tipos de armazenamento, e realocar dados de um local de armazenamento para outro. Se um backup completo ou incremental for executado durante esses procedimentos, o sistema poderá estar no estado intermediário, o que não poderá ser restaurado corretamente mais tarde. Se as configurações dos locais de armazenamento foram alteradas, execute o backup completo novamente antes de realizar o procedimento de restauração. É necessário realizar a reconfiguração do agendamento do backup incremental.

Verificação do backup

A etapa de verificação do backup confirma os dados sujeitos a backup após a conclusão do procedimento de backup.

Esta etapa gera dois relatórios. Ambos os relatórios estão localizados na subpasta Verificação.

- VerificationReport.xml – Este arquivo contém informações técnicas sobre o backup, incluindo informações sobre as entidades sujeitas a backup, tais como arquivos, seus hashes, entidades de bancos de dados etc. Em caso de restauração, este relatório será usado para comparação entre os arquivos e as entidades dos bancos de dados.
- VerificationReport.html – Este relatório contém informações sobre o backup, o número de arquivos verificados, informações sobre verificação de arquivos com falha e os resultados da verificação da entidade do banco de dados em uma visualização legível por humanos.

A etapa de verificação confirma se as entidades principais (arquivos carregados, entidades de banco de dados) foram salvas corretamente. O número de arquivos para verificação é especificado no arquivo de configuração após a configuração do backup (10% ou 10.000 por padrão).

Os arquivos armazenados em localizações no local serão verificados e incluídos no relatório após o procedimento de backup. Os arquivos de locais de armazenamento do AWS S3 não são verificados porque seu backup é feito usando o procedimento AWS e, portanto, não fazem parte da verificação. No caso de uma combinação de armazenamento de arquivos no local e AWS S3, a verificação do arquivo é realizada apenas nos arquivos salvos no sistema de arquivos, e apenas o número total de arquivos no armazenamento seguro salvos no sistema de arquivos são listados e comparados.

Em caso de restauração, todas as entidades incluídas no relatório de backup serão verificadas.

Qualquer entidade (ou sua versão) modificada após o horário inicial do backup não será incluída nos relatórios e não será verificada durante o procedimento de restauração.

NOTA

Quando AWS é escolhido como um local de backup, o relatório de verificação é armazenado localmente em: C:\ProgramData\Agilent\Backup\Verification

Verificação de Arquivos

Para a Verificação de Arquivo, é usada a seguinte lógica:

- O Utilitário de Backup conta, em primeiro lugar, todos os arquivos sujeitos a backup e seleciona aleatoriamente por padrão um mínimo de 10% da quantidade desses arquivos e arquivos de limite superior para verificação. A porcentagem selecionada dos arquivos para verificação é sempre arredondada; por exemplo, para 3 arquivos, 10% corresponde a 0,3, e este valor é arredondado para 1. Isso é útil para uma pequena quantidade dos arquivos no armazenamento seguro, pois a ferramenta garante que, no mínimo, 1 arquivo será verificado.
- Em seguida, o utilitário seleciona uma versão aleatória de cada arquivo. Por exemplo, se um arquivo no armazenamento seguro tiver três revisões (1.0, 2.0 e 3.0), o utilitário selecionará aleatoriamente uma delas.
- A verificação exclui arquivos excluídos.
- O procedimento de verificação compara a soma de verificação e o tamanho dos arquivos sujeitos a backup com as informações do arquivo do armazenamento seguro. Se as somas de verificação forem iguais, a verificação será aprovada. Caso contrário, a verificação será reprovada.

A quantidade de arquivos para verificação pode ser configurada com as seguintes propriedades na seção Backup do arquivo configuration.xml, localizado na pasta %ProgramData%\Agilent\Installation. Você deve ser um Administrador do Sistema para modificar este arquivo.

- PercentFilesVerification – A porcentagem de arquivos verificados (padrão 10%), intervalo de 1 a 100.
- TotalFilesVerificationLimit – Os arquivos de limite superior para verificação (padrão 10.000). Valores negativos e fracionários não são permitidos.

Definir os dois valores como "0" fará com que a verificação do arquivo seja ignorada.

O novo valor é aplicado durante um "Fazer backup agora" na página Processamento antes da primeira etapa e quando um backup é iniciado a partir de um "Backup por agendamento".

Verificação de registros do Shared Services

A verificação inclui verificar o número de registros do banco de dados do Shared Services no momento do backup para:

- Contagem de projetos
- Contagem de instrumentos
- Contagem de usuários
- Contagem de registros de atividades

NOTA

As contas de usuário OLSS para os processos de backup e restauração devem ter a função "Tudo" atribuída.

Se uma das contas de usuário OLSS para backup e restauração não tiver todos os privilégios necessários (por exemplo, o usuário OLSS usado durante o backup não tem acesso aos instrumentos, mas o usuário OLSS usado na restauração tem acesso aos instrumentos), a verificação da restauração falhará porque no relatório de verificação do backup a contagem de instrumentos será 0, mas no relatório de verificação da restauração não será zero se houver alguns instrumentos no banco de dados.

Quando um backup for realizado, as informações de contagem do registro de atividades serão aplicadas ao relatório de verificação. O número de registros que serão considerados no relatório será atualizado até a data e hora de início do backup. Apenas as primeiras 10.000 entradas no registro de atividades serão consideradas na verificação.

Backup incremental de bancos de dados PostgreSQL

O backup incremental cumulativo é um processo que salva arquivos de dados e objetos que foram modificados desde o último backup completo. Trata-se de uma técnica de backup de dados que atualiza apenas os dados modificados, em vez dos dados completos. Realize essas etapas no servidor do banco de dados PostgreSQL.

O PostgreSQL não possui uma ferramenta que realize backup incremental, mas possui uma estratégia de backup incremental. Essa estratégia significa que você pode combinar um backup no nível do sistema de arquivos com um backup dos arquivos WAL.

Para recuperar com sucesso usando o Arquivamento Contínuo (também chamado de "backup online" por muitos fornecedores de banco de dados), você precisa de uma sequência contínua de arquivos WAL arquivados que se estenda pelo menos até o horário inicial do seu backup. Para começar, configure o procedimento de arquivamento de arquivos WAL seguindo o procedimento em "[Configurar backup incremental usando a Ferramenta de Configuração Incremental](#)" na página 55 antes de fazer o primeiro backup de base.

Configurar backup incremental usando a Ferramenta de Configuração Incremental

A Ferramenta de Configuração Incremental configura automaticamente o suporte de backup incremental. Ela permite que você configure todas as instâncias do PostgreSQL usadas pelo OpenLab Server/ECM XT de uma só vez. A Ferramenta de Configuração Incremental executa as seguintes ações:

- Atualiza as configurações para suporte dos backups incrementais do PostgreSQL.
- Requer uma reinicialização dos serviços PostgreSQL após a atualização.
- Atualiza o arquivo BackupUtility.config para oferecer suporte a backups incrementais pelo Utilitário de Backup.

A ferramenta está localizada por padrão em C:\Program Files (x86)\Agilent Technologies\OpenLab Backup Utility\Incremental Config Tool\PgIncrementalConfigTool.exe.

O PgIncrementalConfigTool pode ser executado a partir da linha de comando. Execute o PgIncrementalConfigTool como administrador e configure as credenciais de acesso de acordo com **"Reconfigurar as Credenciais de Acesso"** na página 61

Parâmetros:

- -on – obrigatório, habilitar backup incremental, configurar caminhos padrão
- -off – obrigatório, desabilitar backup incremental
- -olcmWalDir <caminho> – opcional, configura o caminho definido para PostgreSQL do OLCM, aplicável apenas com parâmetro on

Por exemplo,

PgIncrementalConfigTool.exe -on

Habilite o backup incremental, configure os caminhos padrão.

PgIncrementalConfigTool.exe -off

Desabilite o backup incremental.

PgIncrementalConfigTool.exe -on -olcmWalDir D:\wal\olcm "D:\wal\dr files"

Habilite o backup incremental, configure os caminhos especificados.

Saída de ferramenta

A ferramenta configura os bancos de dados PostgreSQL dependendo da topologia, reinicia os serviços PostgreSQL e exibe a mensagem "Configuração concluída com sucesso".

Em caso de erros, ela exibe "PgIncrementalConfigTool falhou. Arquivos de registro: <log file path>"

Configurar o diretório de dados personalizado do banco de dados PostgreSQL

- 1 Obtenha a configuração atual do serviço PostgreSQL.
 - a Execute a linha de comando e, na máquina onde o banco de dados PostgreSQL está instalado, execute o seguinte comando: `sc qc postgresql-x64-15-dr`.
 - b O próximo valor após a opção -D mostra a localização atual dos dados.
- 2 Pare o serviço PostgreSQL: `postgresql-x64-15-dr`.
- 3 Mover conteúdo do local de dados atual para o novo local.
- 4 Modificar as configurações do serviço PostgreSQL com base no arquivo atual. Configurar uma nova localização de dados. Por exemplo: `sc config postgresql-x64-15-dr binPath= "C:\Program Files (x86)\PostgreSQL\15\bin\pg_ctl.exe" runservice -N \"postgresql-x64-15-dr\" -D \"E:\NewDataLocation\" -w`
- 5 Atualize o valor do registro para o serviço PostgreSQL. Configurar a nova localização dos dados para:
 - Computer\HKEY_LOCAL_MACHINE\SOFTWARE\PostgreSQL\FB5FABF4-6023-4975-A98D-A435C547CAC1\Installations\postgresql-x64-15
 - HKEY_LOCAL_MACHINE\SOFTWARE\PostgreSQL\FB5FABF4-6023-4975-A98D-A435C547CAC1\Services\postgresql-x64-15\DataDirectory
- 6 Inicie o serviço PostgreSQL: `postgresql-x64-15-dr`
- 7 Reinicialize o computador.

Restaurar o OpenLab Server/ECM XT Usando o Utilitário de Restauração

Use esses procedimentos para restaurar seu sistema a partir de um backup existente se o servidor OpenLab Server/ECM XT ficar inoperável devido a uma falha de hardware ou software.

O procedimento de restauração restaurará apenas os dados confirmados capturados pelo procedimento de backup bem-sucedido. Quaisquer dados colocados em espera para carregar e que ainda não foram confirmados ou que foram adicionados ou atualizados após a realização do backup não serão recuperados por meio da restauração de um backup.

CUIDADO

Certifique-se de que o sistema de restauração tenha a mesma atualização do OpenLab Server/ECM XT que o sistema onde o backup foi criado.

CUIDADO

Nos casos em que um sistema restaurado será executado ao mesmo tempo que o sistema de origem (onde o backup foi feito), assegure-se de que o sistema restaurado esteja em uma rede isolada do sistema de origem. Por exemplo, se um sistema de teste for criado a partir de um backup do sistema de produção, ele deverá estar em uma rede isolada do sistema de produção. Se o sistema de teste e o sistema de produção estiverem na mesma rede, isso pode fazer com que os dois servidores criem um cluster e interajam entre si. Isso pode fazer com que os dados fiquem corrompidos e sejam perdidos.

Verificação

Ao restaurar para uma instalação existente, também é possível verificar se a restauração foi realizada corretamente. Os relatórios de verificação são salvos em C:\ProgramData\Agilent\Restore\Verification.

Solução de problemas do procedimento de restauração

O Utilitário de Restauração coleta logs na pasta "%ProgramData%\Agilent\LogFiles\Restore". Durante o procedimento de restauração, todas as etapas são verificadas e todo o procedimento de restauração será interrompido na primeira etapa falhada. Um link com a etapa falhada abre o arquivo de registro de restauração atual para ajudar a identificar a causa raiz do problema. Durante a configuração de restauração, as validações em cada página evitam possíveis erros com credenciais incorretas, nenhum acesso ao conteúdo e locais de arquivo, formato incorreto e outros problemas de configuração comuns.

Restaurar um sistema com banco de dados PostgreSQL ou Microsoft SQL

Use o Utilitário de Restauração para restaurar um sistema OpenLab Server/ECM XT suportado com um banco de dados PostgreSQL ou do servidor MS SQL. Para obter uma lista das topologias suportadas pelo Utilitário de Restauração, consulte **"Usar os Utilitários de Backup e Restauração"** na página 46.

Em todos os outros casos, siga o procedimento de restauração manual descrito em **"Procedimento Manual de Restauração do Servidor de Aplicativos OpenLab Server/ECM XT"** na página 68.

Durante o procedimento de restauração, as validações em cada página evitam possíveis erros, como credenciais incorretas, nenhum acesso ao conteúdo e locais de arquivo, formatos incorretos e outros problemas de configuração comuns.

Para topologias suportadas, use o seguinte procedimento para restaurar seu sistema usando o Utilitário de Restauração.

CUIDADO

O mesmo nível de atualização do OpenLab Server/ECM XT deve estar instalado, como no sistema onde o backup foi criado. Isso é necessário para garantir que o nível de patch do banco de dados restaurado corresponda ao nível de patch do aplicativo.

NOTA

O Utilitário de Restauração pode restaurar um sistema a partir de backups cold e hot criados com o Utilitário de Backup. O Utilitário de Restauração pode ser executado em sistemas com o OpenLab Server/ECM XT instalado (consulte **"Reconfiguração durante a restauração"** na página 60).

NOTA

O Utilitário de Restauração não restaura certificados personalizados usados para uma conexão segura. Após a restauração, o sistema será configurado com certificados internos. Para configurar certificados personalizados, consulte **"Protegendo o Sistema"** na página 23.

NOTA

Se você estiver usando o Sample Scheduler, os serviços do Sample Scheduler deverão ser reiniciados após o procedimento de restauração.

NOTA

Se você estiver usando caminhos não padrão para configurar o PostgreSQL para backup incremental em um sistema com backup, siga as instruções em **"Configurar backup incremental usando a Ferramenta de Configuração Incremental"** na página 55 após a restauração.

NOTA

Se você instalar o OpenLab em um novo sistema antes de restaurar um backup dele, o sistema recém-instalado deverá ter a mesma configuração do sistema com backup. Por exemplo, se o sistema com backup foi configurado com autenticação por domínio, configure o sistema recém-instalado com autenticação por domínio e mapeie os mesmos usuários Administradores. Isso garantirá que a restauração seja bem-sucedida.

Usar o Utilitário de Restauração para sistemas com OpenLab Server/ECM XT instalado

Use o procedimento a seguir para restaurar um sistema instalado anteriormente cujo backup foi feito usando o Utilitário de Backup.

CUIDADO

Interrompa todas as operações do OpenLab Server/ECM XT antes de realizar o processo de restauração. Certifique-se de que todos os clientes, instrumentos ou outras partes do sistema não estejam usando o servidor durante o processo de restauração.

Restaurar para uma instalação existente usando o Utilitário de Restauração

Etapas	Opções	Observações
1 Inicie o Utilitário de Restauração em Iniciar > Agilent Technologies > Utilitário de Restauração.		Você deve ter privilégios de administrador do sistema para executar o Utilitário de Restauração.
2 Na página Configuração de Restauração, selecione a localização do backup.	<ul style="list-style-type: none"> Selecione Sistema de arquivo como a localização do backup se o backup estiver localizado localmente ou no compartilhamento do Windows. Selecione a pasta de backup usada pelo Utilitário de Backup e clique em Próximo. Selecione AWS S3 como Localização do backup se o backup estiver localizado no armazenamento do Amazon AWS S3. Especifique o nome, a área de armazenamento do backup do AWS S3 e as chaves e, em seguida, clique em Próximo. A opção Restauração e verificação parcial está selecionada por padrão e isso não inclui a verificação do registro de atividades. Para a verificação do registro de atividades e a recriação do índice do registro de atividades, selecione a opção Restauração e verificação completa. 	<ul style="list-style-type: none"> O Utilitário de Restauração primeiro restaura o backup completo da pasta Atual e, em seguida, restaura todos os backups incrementais da pasta Incremental. Os relatórios de verificação são salvos em C:\ProgramData\Agilent\Restore\Verification. A verificação está disponível apenas para sistemas nos quais o software OpenLab já tenha sido instalado. Se a opção Verificar apenas for selecionada, a próxima página será Revisão e, em seguida, Processamento.
3 As configurações da página Credenciais do Shared Services são pré-preenchidas com base no sistema cujo backup foi feito.	<ul style="list-style-type: none"> Se o estado do ambiente atual mudou desde o backup, modifique essas configurações. Clique em Validar para confirmar que as credenciais inseridas são válidas. 	<ul style="list-style-type: none"> Essas credenciais são solicitadas por padrão do arquivo configuration.xml. Essa página é ignorada se a opção Apenas Restaurar estiver selecionada. Em outros casos, esta página é exibida para os backups criados nos sistemas com tipo de autenticação de Domínio OLSS.
4 As configurações da página Servidor do Banco de Dados são pré-preenchidas com base no sistema sujeito a backup.	<ul style="list-style-type: none"> Se o estado do ambiente atual mudou desde o backup, modifique essas configurações. Para o SQL Server, forneça o nome do servidor e as credenciais do administrador do banco de dados. Para PostgreSQL, forneça configurações de conexão e credenciais de administrador do banco de dados. Para obter mais informações sobre a reconfiguração durante a restauração, consulte "Reconfiguração durante a restauração" na página 60 	
5 As configurações da página Credenciais de Acesso são pré-preenchidas com base no sistema feito o backup.	<ul style="list-style-type: none"> Se o estado do ambiente atual mudou desde o backup, modifique essas configurações. Clique em Verificar para confirmar que as credenciais inseridas são válidas. 	
6 Revise as configurações e clique em Aplicar.		

Restaurar para uma instalação existente usando o Utilitário de Restauração (continuação)

Etapas	Opções	Observações
7 É possível acompanhar o progresso do procedimento de restauração na página Restaurar.	Quando solicitado na etapa Executar Utilitário de Configuração do Servidor, insira as credenciais de administrador do Shared Services.	Se você tiver selecionado Restauração e Verificação Parcial, Restauração e Verificação Completa ou Apenas Verificar, uma etapa de verificação será exibida como a última etapa. Clique no link "concluído" do status de verificação para abrir o relatório de verificação.
8 Após a conclusão do procedimento de restauração, clique em Concluído.		
9 Reinicie o sistema após a restauração.	Clique em Sim para reinicializar o sistema imediatamente. Clique em Não para adiar a reinicialização e reinicie-o manualmente.	A reinicialização do sistema é recomendada após uma restauração concluída em um sistema já instalado.
10 Execute a Etapa 6 – Etapa 7, começando na página 72 .		

Reconfiguração durante a restauração

A reconfiguração poderá ser necessária:

- Se o servidor com o banco de dados tiver sido movido para outro computador
- Se a porta ou as credenciais administrativas tiverem sido alteradas
- Se um usuário restaurar o backup de outro servidor
- Se um banco de dados for movido para outra instância no servidor
- Se os locais de armazenamento tiverem sido alterados
- Se o caminho de indexação do Content Management tiver sido alterado

É possível reconfigurar as configurações do PostgreSQL e do MS SQL durante o procedimento de restauração. Na página Servidor do Banco de Dados, são exibidas as informações pré-carregadas sobre a conexão com um banco de dados. Se você alterar algo nesta página, confirme se as informações estão corretas. O utilitário verificará os valores e exibirá uma mensagem com os detalhes caso ocorra algum problema.

Reconfigurar um servidor do banco de dados PostgreSQL

Na página Servidor do Banco de Dados é possível alterar e verificar o nome do servidor, a porta, o superusuário e a senha. Se outro usuário for usado, ele deverá ter os mesmos privilégios do superusuário-padrão (postgres).

Para verificar os valores inseridos, clique em **Verificar** ou **Próximo**.

Reconfigurar um servidor do banco MS SQL

Na página Servidor do Banco de Dados é possível alterar e verificar o nome do servidor, a instância nomeada, a porta, o superusuário e a senha. Se outro usuário for usado, ele deverá ter os mesmos privilégios do superusuário-padrão (sa).

Uma instância nomeada é o nome que um usuário especifica ao instalar o MS SQL Server (se for diferente do padrão).

Para usar o usuário do Windows, ele deverá ser adicionado às configurações de segurança do MS SQL Server. Consulte a seção Guia de Instalação do OpenLab Server/ECM XT em Configurar um Servidor de Banco de Dados Remoto.

Para verificar os valores inseridos, clique em **Verificar** ou **Próximo**.

Reconfigurar as Credenciais de Acesso

Nesta página, é possível alterar uma conta que tenha sido usada para acessar todos os caminhos de armazenamento de conteúdo. Certifique-se de que esta conta esteja no Grupo administrador nas máquinas do servidor ECM XT e do servidor do banco de dados.

Não são suportadas contas separadas para locais de armazenamento individuais.

Certifique-se de que o usuário tenha a permissão "Logon como um serviço".

Para verificar os valores inseridos, clique em **Verificar** ou **Próximo**.

Revisar e iniciar a restauração

Na página Revisão, revise o resumo das configurações do OpenLab Server que você está configurando.

Se tudo estiver correto, clique em **Aplicar** para iniciar o processo de restauração. Clique em **Voltar** se pretender alterar algo.

Procedimentos Manuais de Cold Backup e Restauração

Procedimento Manual de Backup do Servidor de Aplicativos OpenLab Server/ECM XT 63

Fazer um backup manual do sistema 63

Procedimento Manual de Restauração do Servidor de Aplicativos OpenLab Server/ECM XT 68

Procedimento Manual de Backup do Servidor de Aplicativos OpenLab Server/ECM XT

O backup periódico de cada servidor de aplicativos OpenLab Server/ECM XT é obrigatório. Os administradores do servidor OpenLab Server/ECM XT devem criar backups completos periódicos e backups diferenciais entre os backups completos. Esses backups são a única forma de restaurar um servidor OpenLab Server/ECM XT caso ocorra uma falha de hardware ou software.

O backup apenas reduz a quantidade de perda de dados caso ocorra uma falha de sistema catastrófica. A realização de backups garante que todos os dados confirmados no momento do backup podem ser restaurados. Quaisquer dados colocados em espera para carregar e que ainda não foram confirmados, adicionados ou atualizados no sistema após a realização do backup não serão recuperáveis por meio de restauro de um backup.

Também é obrigatório testar os procedimentos de restauração ("**Procedimento Manual de Restauração do Servidor de Aplicativos OpenLab Server/ECM XT**" na página 68) para garantir que os backups sejam realizados de forma apropriada e que possam ser usados para uma restauração. Para uma restauração eficaz, deve ser criado um plano de recuperação de desastres.

O OpenLab Server/ECM XT armazena arquivos e índices no sistema de arquivos do seu servidor. O local dessa pasta é determinado quando o produto é instalado. Outros dados, como informações da pasta, registros de auditoria e assinaturas, são armazenados em um banco de dados relacional.

Um backup completo captura um conjunto completo de dados no OpenLab Server/ECM XT, incluindo arquivos carregados e seus bancos de dados. Um backup diferencial contém alterações que ocorreram desde o último backup completo. O processo do backup diferencial é mais rápido que o do backup completo, uma vez que são copiados apenas os elementos modificados.

Se estiver atualizando o seu servidor, realize os seguintes procedimentos na sua máquina antes de atualizar. Todas as áreas de trabalho e filas de upload de arquivos devem ser limpas antes do procedimento de atualização. Não se deve ter dados em nenhuma das filas ao realizar a atualização para um SO diferente. Todos os uploads de arquivos devem estar concluídos. A fila de upload do buffer de arquivo deve estar limpa antes da atualização.

Fazer um backup manual do sistema

Etapa 1 Determinar pastas de índices, conteúdo e banco de dados

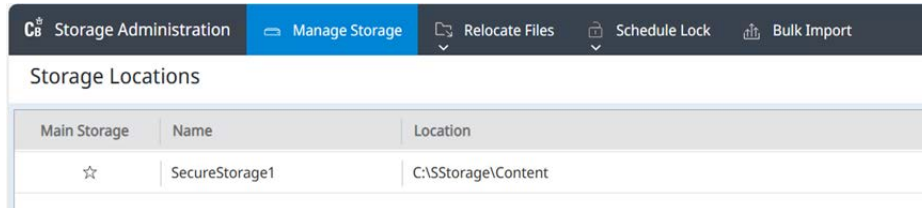
Para realizar o backup e restauração do OpenLab Server/ECM XT, você precisa saber o nome dos seus bancos de dados, o local da pasta de conteúdo armazenado, o local da pasta de índices armazenados e outras informações de instalação e configuração.

Existem dois bancos de dados que precisam de backup. O banco de dados do servidor OpenLab Server/ECM XT e o banco de dados Shared Services. Os nomes desses bancos de dados podem ser recuperados do respectivo utilitário de administração do banco de dados (por exemplo, pgadmin4, SQL Server Management Studio).

De forma similar, o caminho da pasta de conteúdo principal (padrão) também é um parâmetro que é especificado durante a instalação do servidor. Poderá haver locais adicionais de armazenamento definidos após a instalação inicial. Use o procedimento a seguir para determinar esses caminhos.

- 1 Vá até a máquina do OpenLab Server/ECM XT e faça login com uma conta de Administrador.
- 2 Abra o URL: <https://localhost/openlab-storage-admin/> e faça login com uma conta administrativa.

Uma página da Web é exibida e fornece os caminhos para os locais de armazenamento seguro. A localização padrão é C:\SStorage\Content.



Main Storage	Name	Location
☆	SecureStorage1	C:\SStorage\Content

Etapa 2 Silenciar o sistema e parar serviços do OpenLab Server/ECM XT:

- 1 Abra os **Serviços do Windows** (services.msc) e **Pare o serviço**: Serviço de Download e Upload do Agilent OpenLab SDMS.
- 2 Abra um navegador da Web e acesse o URL:
<https://localhost:15671/openlab/rabbitmq/#/queues>
- 3 Faça login na fila de mensagens RabbitMQ como o usuário **drradmin**.
- 4 Na guia **Filas**, verifique se a fila **metadata.requests.persistence.new** e a fila **metadata.requests.extraction.new** estão ociosas.
- 5 Prossiga com a interrupção dos serviços:
 - Agilent OpenLab Shared Services
 - Serviço de certificados
 - Todos os serviços do SDMS OpenLab
 - Todos os serviços relacionados ao repositório de dados
 - OpenSearch 2.5.0 (opensearch-service-x64)
 - PostgreSQL 15.1.1.80 (x64) (somente aplicável ao usar o banco de dados PostgreSQL para o OpenLab Server/ECM XT). Ignore este serviço se o banco de dados estiver em um host separado.
 - RabbitMQ

NOTA

Se sua topologia tiver vários servidores de aplicativos OpenLab Server/ECM XT, estes serviços deverão ser interrompidos em todos os servidores de aplicativos.

Abaixo estão comandos de exemplo que podem ser executados usando uma janela de comando do Windows (com privilégios de administrador) ou um arquivo em lote. Estes comandos interromperão todos os serviços relevantes do OpenLab.

```
REM Estes comandos interrompem todos os serviços relevantes do OpenLab CDS para
que um cold backup possa ser realizado
net stop "Agilent OpenLab Activity Log Service"
net stop "Agilent OpenLab Audit Trail Service"
net stop "AutomationServerHost"
net stop "Agilent OpenLab Backup Monitoring Service"
net stop "Agilent OpenLab Backup Notification Service"
```



```

net stop "Agilent OpenLab Backup Task Status Cache Service"
net stop "OpenLabCertificateService"
net stop "DataCollectionAgent"
net stop "DataCollectionService"
net stop "DataRepositoryBaseService"
net stop "Agilent OpenLab Distributed Transaction Coordinator Service"
net stop "Agilent OpenLab Electronic Signature Service"
net stop "Agilent OpenLab License Server"
net stop "Agilent OpenLab Licensing Support"
net stop "Agilent OpenLab CopyTo Server"
net stop "DiagnosticsToolsService"
net stop "AuthenticationService"
net stop "BrowsingService"
net stop "BulkImportService"
net stop "ContentBrowserService"
net stop "DeleteService"
net stop "UploadDownloadService"
net stop "Agilent OpenLab SDMS Action Service"
net stop "SDMS_MetadataExtractionService"
net stop "SDMS_MetadataPersistenceService"
net stop "SDMS_MetadataQueryService"
net stop "PermissionsSyncService"
net stop "SecureStorageAdministrationService"
net stop "StorageConfigurationService"
net stop "StorageManagementService"
net stop "SharedServicesHost"
net stop "Agilent.Scheduler.Webserver"
net stop "Agilent Sample Scheduler Database Management Agent"
net stop "Agilent Sample Scheduler Services Controller"
net stop "Agilent.Scheduler.Lims.Agent"
net stop "Agilent.Scheduler.Orchestrator"
net stop "Agilent.TestServices.WebService"
net stop "Agilent.TestServices.Server.Main"
net stop "OpenLabReverseProxy"
net stop "opensearch-service-x64"
net stop "RabbitMQ"
net stop "postgresql-x64-15-dr"

```

Etapa 3 Fazer backup dos bancos de dados

Esta seção fornece uma abordagem simples e interativa para fazer o backup dos bancos de dados. Consulte a documentação do PostgreSQL ou do MS SQL Server para conhecer outras opções, algumas das quais também permitem automatizar o processo.

Procedimento para PostgreSQL O local no qual os arquivos de banco de dados estão armazenados é especificado durante a instalação do servidor. No caso do banco de dados PostgreSQL local, por padrão, é C:\ProgramData\Agilent\OpenLab Platform\PostgreSQL.

Faça o backup do banco de dados PostgreSQL copiando a pasta do banco de dados (C:\ProgramData\Agilent\OpenLab Platform\PostgreSQL) usando o **Backup do Windows Server** ou qualquer outra ferramenta de sua escolha.

NOTA

Ao usar o **Backup do Windows Server**, só é possível restaurar na mesma máquina, com o mesmo nome de computador. Para restaurar em um computador diferente, use uma ferramenta ou procedimento diferente.

Como alternativa, use a ferramenta de linha de comando "pg_basebackup" do PostgreSQL. Usar essa ferramenta requer uma instância de banco de dados em execução. Para obter mais informações, consulte a documentação online do PostgreSQL.

Procedimentos para o MS SQL Server Verifique se o serviço do MSSQL foi iniciado. Use o **SQL Server Management Studio** para fazer backup do banco de dados Shared Services (o padrão é OLSharedServices), do banco de dados do servidor OpenLab Server/ECM XT (o padrão é datarepo) e do banco de dados do Sample Scheduler (o padrão é OpenLabScheduler<version>). A ferramenta permite aos usuários realizar **Backups completos** e também **Backups diferenciais**.

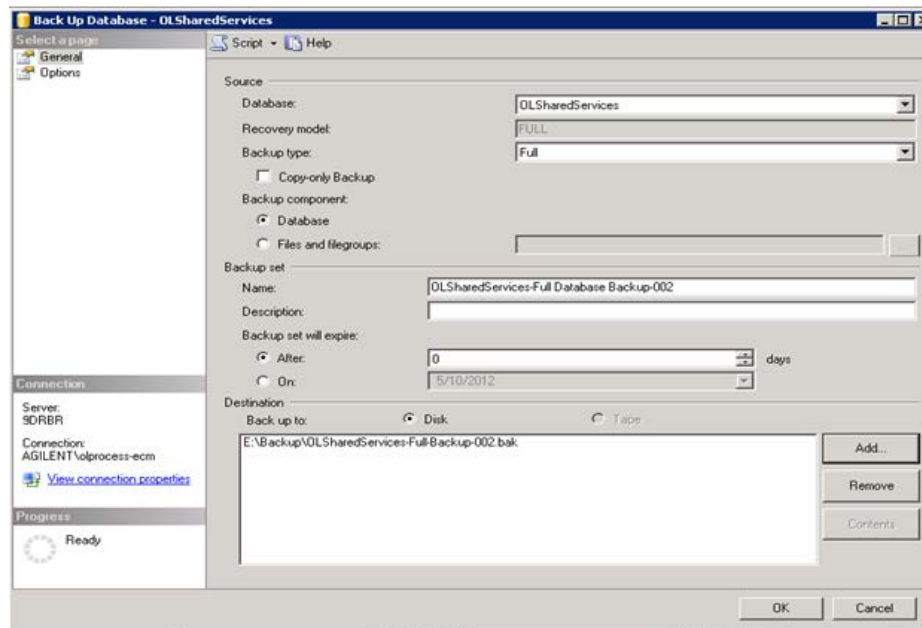


Figura 1. Usando o SQL Server Management Studio para backup

Etapa 4 Fazer backup de pastas de conteúdo

Use o **Backup do Windows Server** ou qualquer outra ferramenta de sua escolha para fazer backup das pastas de conteúdo do OpenLab Server/ECM XT, conforme determinado em "**Etapa 1 Determinar pastas de índices, conteúdo e banco de dados**" na página 63.

NOTA

Ao usar o **Backup do Windows Server**, só é possível restaurar na mesma máquina, com o mesmo nome de computador. Para restaurar em um computador diferente, use uma ferramenta ou procedimento diferente.

Etapa 5 Fazer backup das informações de configuração do servidor OpenLab Server/ECM XT

Faça backup de todos os arquivos e subpastas dos seguintes diretórios:

- %ProgramData%\Agilent\Installation
- %ProgramData%\Agilent\OpenLab Certificate Service
- %ProgramData%\Agilent\OpenLab Platform\OpenSearch
- %ProgramData%\Agilent\OpenLab Platform\Reverse Proxy

Quando o processo de backup tiver terminado, reinicie o servidor.

Comandos de exemplo de backup manual de todos os dados e arquivos de um OpenLab Server

Abaixo estão comandos de exemplo que podem ser executados usando uma janela de comando do Windows (com privilégios de Administrador) ou um arquivo em lote. Os comandos devem ser alterados para corresponder ao local de backup escolhido. Ao copiar/colar, remova o CRLF das linhas.

```
REM Comandos para um arquivo em lote do Windows para fazer backup manual de
arquivos de configuração, BD e dados de gestão de conteúdo
REM Precisa ser executado como Administrador
REM Nos exemplos abaixo, todos os dados têm o backup feito em várias pastas na
unidade E:
REM
REM Certifique-se de que a pasta para o arquivo de registro existe (p. ex.:
C:\temp)
REM Copie os arquivos de instalação e configuração do OpenLab
robocopy "%ProgramData%\Agilent\Installation" "E:\ProgramData\Installation" /e
/zb /log:C:\temp\olcopy.log
robocopy "%ProgramData%\Agilent\OpenLab Certificate Service"
"E:\ProgramData\OpenLab Certificate Service" /e /zb /log+:C:\temp\olcopy.log
robocopy "%ProgramData%\Agilent\OpenLab Platform\Reverse Proxy"
"E:\ProgramData\Reverse Proxy" /e /zb /log+:C:\temp\olcopy.log
REM
REM Backup de índice do OpenSearch
robocopy "%ProgramData%\Agilent\OpenLab Platform\OpenSearch"
"E:\ProgramData\OpenSearch" /e /zb /log+:C:\temp\olcopy.log
REM
REM Copie os arquivos do BD PostgreSQL - requer o encerramento prévio do
serviço do banco de dados
robocopy "%ProgramData%\Agilent\OpenLab Platform\PostgreSQL"
"E:\ProgramData\PostgreSQL" /e /zb /log+:C:\temp\olcopy.log
REM
REM Abordagem alternativa para copiar um BD PostgreSQL, que também funciona
enquanto o BD está em execução
REM Isto requer que as credenciais de login do usuário Administrador do BD
estejam disponíveis
REM pode ser necessário adicionar as seguintes linhas (s/ REM) ao arquivo:
REM %ProgramData%\Agilent\OpenLab Platform\PostgreSQL\15\data\pg_hba.conf
REMhost      replication  postgres  127.0.0.1/32      md5
REMhost      replication  postgres  ::1/128          md5
REM
REM Instância de backup concluído - Comando:
REM "C:\Program Files (x86)\PostgreSQL\15\bin\pg_basebackup.exe" -U postgres -W
-p 5432 -D "E:\ProgramData\PostgreSQL" --wal-method=stream --format=tar -z
--progress --no-manifest -l "Manual Full-backup"
REM
REM Copie o armazenamento de conteúdo da gestão de conteúdo eletrônico (em
vários threads para um backup mais rápido)
robocopy "C:\SStorage" "E:\SStorage" /e /zb /mt:4 /log+:C:\temp\olcopy.log
```

Revise o arquivo de registro quanto a divergências ou arquivos ignorados ou com falhas

Procedimento Manual de Restauração do Servidor de Aplicativos OpenLab Server/ECM XT

Use esses procedimentos para restaurar seu sistema a partir de um backup existente se o servidor de aplicativos OpenLab Server/ECM XT ficar inoperável devido a uma falha de hardware ou software.

Se estiver atualizando o seu servidor, realize os seguintes procedimentos na sua máquina depois de atualizar.

O procedimento de restauração restaurará apenas os dados confirmados capturados pelo procedimento de backup bem-sucedido. Quaisquer dados colocados em espera para carregar e que ainda não foram confirmados, adicionados ou atualizados no sistema após a realização do backup não serão recuperáveis por meio de restauro de um backup.

Etapas 1 Instalar o OpenLab Server/ECM XT usando a configuração original

Siga os procedimentos de instalação para instalar e configurar um novo OpenLab Server/ECM XT na máquina. A nova instalação deve ter o mesmo nível de patch do sistema cujo backup foi feito. O procedimento a seguir descreve como instalar o OpenLab Server/ECM XT utilizando informações restauradas através de um banco de dados PostgreSQL como exemplo. O procedimento é semelhante para outros bancos de dados.

- 1 Execute a **Etapas 1 – Instalar ou atualizar pré-requisitos do software** a partir do instalador.
- 2 Na tela **Tipo de Banco de Dados**, verifique se **PostgreSQL Server** está selecionado e clique em **Próximo**.
- 3 Na tela **PostgreSQL**, mantenha a Porta e o Nome do Servidor padrão e clique em **Próximo**.
- 4 Na tela **Configurações do PostgreSQL**, atualize o local do Banco de Dados PostgreSQL para corresponder ao local do servidor de origem. Use a mesma senha de super usuário e clique em **Próximo**.
- 5 Na tela **Credenciais de Serviço** use a mesma senha de serviço de componente que foi usada no servidor cujo backup foi feito. prossiga pelas próximas telas até que a instalação seja concluída e clique em **Concluir**.
- 6 Execute a **Etapas 2 – Criar ou Atualizar Esquema de Banco de Dados** a partir do instalador.
- 7 Na tela **Servidor de Banco de Dados**, selecione **Criar um novo banco de dados para o OpenLab Server** e clique em **Próximo**.
- 8 Termine a configuração do esquema do banco de dados.
- 9 Execute a **Etapas 3 – Instalar ou atualizar o servidor OpenLab Server/ECM XT**.
- 10 Execute a **Etapas 4 – Configurar ou reconfigurar o servidor OpenLab Server/ECM XT**.
Tenha disponíveis as credenciais de administrador do Shared Services durante essa etapa.
- 11 Na tela **Locais de Armazenamento**, verifique se o caminho e o nome do local de armazenamento correspondem aos locais reais das pastas de dados. Clique em **Verificar** e, em seguida, clique em **Próximo**.
- 12 Revise o resumo geral da configuração atentamente. Se estiver OK, clique em **Aplicar**.
- 13 Feche as janelas do instalador.

Etapa 2 Encerrar todos os serviços do OpenLab

Abra os **Serviços do Windows** (services.msc) e **Pare os serviços**:

- Agilent OpenLab Shared Services
- Certificate service
- Test services
- Todos os serviços do SDMS OpenLab
- Todos os serviços relacionados ao repositório de dados
- OpenSearch 2.5.0 (opensearch-service-x64)
- PostgreSQL 15.1.1.80 (x64) (somente aplicável ao usar o banco de dados PostgreSQL para o OpenLab Server/ECM XT). Ignore este serviço se o banco de dados estiver em um host separado.
- RabbitMQ

Abaixo estão comandos de exemplo que podem ser executados usando uma janela de comando do Windows (com privilégios de Administrador) ou um arquivo em lote. Estes comandos interromperão todos os serviços relevantes do OpenLab.

REM Estes comandos interrompem todos os serviços relevantes do OpenLab CDS para que um cold backup possa ser realizado

```
net stop "Agilent OpenLab Activity Log Service"
net stop "Agilent OpenLab Audit Trail Service"
net stop "AutomationServerHost"
net stop "Agilent OpenLab Backup Monitoring Service"
net stop "Agilent OpenLab Backup Notification Service"
net stop "Agilent OpenLab Backup Task Status Cache Service"
net stop "OpenLabCertificateService"
net stop "DataCollectionAgent"
net stop "DataCollectionService"
net stop "DataRepositoryBaseService"
net stop "Agilent OpenLab Distributed Transaction Coordinator Service"
net stop "Agilent OpenLab Electronic Signature Service"
net stop "Agilent OpenLab License Server"
net stop "Agilent OpenLab Licensing Support"
net stop "Agilent OpenLab CopyTo Server"
net stop "DiagnosticsToolsService"
net stop "AuthenticationService"
net stop "BrowsingService"
net stop "BulkImportService"
net stop "ContentBrowserService"
net stop "DeleteService"
net stop "UploadDownloadService"
net stop "Agilent OpenLab SDMS Action Service"
net stop "SDMS_MetadataExtractionService"
net stop "SDMS_MetadataPersistenceService"
net stop "SDMS_MetadataQueryService"
net stop "PermissionsSyncService"
net stop "SecureStorageAdministrationService"
net stop "StorageConfigurationService"
net stop "StorageManagementService"
net stop "SharedServicesHost"
net stop "Agilent.Scheduler.Webserver"
net stop "Agilent Sample Scheduler Database Management Agent"
net stop "Agilent Sample Scheduler Services Controller"
```

```
net stop "Agilent.Scheduler.Lims.Agent"
net stop "Agilent.Scheduler.Orchestrator"
net stop "Agilent.TestServices.WebService"
net stop "Agilent.TestServices.Server.Main"
net stop "OpenLabReverseProxy"
net stop "opensearch-service-x64"
net stop "RabbitMQ"
net stop "postgresql-x64-15-dr"
```

Etapa 3 Restaurar os bancos de dados

Procedimento para um PostgreSQL Server Determine a pasta do seu banco de dados (por exemplo, "%ProgramData%\Agilent\OpenLab Platform\PostgreSQL) e restaure os bancos de dados PostgreSQL nessa pasta a partir do seu backup. É recomendado manter os caminhos originais para simplificar configurações posteriores.

Procedimento para um MS SQL Server Use esses procedimentos para restaurar o banco de dados e modificar as configurações para cada banco de dados restaurado.

Restaurar bancos de dados

Restaure o banco de dados do Shared Services (OLSharedServices), o banco de dados do servidor OpenLab Server/ECM XT (datarepo) e o banco de dados do Sample Scheduler (OpenLabScheduler) usando o SQL Management Studio.

Definir as configurações do banco de dados do Shared Services usando o SQL Management Studio

- 1 Verifique o usuário do banco de dados no **banco de dados do Shared Services > Segurança > Usuários**. (Reveja os usuários para reutilizar o usuário existente. Caso o banco de dados tenha sido restaurado para um novo servidor, remova o servidor existente. Ele será recriado na próxima etapa.)
- 2 Verifique os logins do MS SQL Server.
 - a Acesse **Segurança > Logins**.
 - b Caso o banco de dados tenha sido restaurado para um novo servidor, remova o usuário do banco de dados OLSS e crie um novo.
 - Autenticação no servidor SQL.
 - A senha não expira. Use a mesma senha usada antes da restauração.
 - Mapeie o novo login do banco de dados **OLSharedServices** com nome de usuário (o padrão é **Olss**) e o esquema padrão é **dbo**.
- 3 Verifique as propriedades do usuário do banco de dados em Banco de dados do **Shared Services > Segurança > Usuários** e modifique a participação do usuário para a função **db_owner**.

Certifique-se de que o login do Shared Services esteja presente no MS SQL Server (crie-o, se necessário).

Se a autenticação do MS SQL Server foi usada na Etapa 2 do procedimento de instalação, certifique-se da existência do login usado nessa etapa.

Se a autenticação do Windows foi usada na Etapa 2 do procedimento de instalação, verifique os seguintes logins predefinidos:

- Para o banco de dados local do MS SQL Server (MS SQL Server e ECM XT Server estão instalados na mesma máquina), use o login "NT AUTHORITY\SYSTEM".

- Para o banco de dados remoto do MS SQL Server (MS SQL Server e ECM XT Server estão instalados em duas máquinas diferentes), use o login "DOMAIN\ECM XT Server machine name\$" do Windows. (Por exemplo, se o domínio for Agilent e o ECM XT Server estiver instalado na máquina "ECMServer", então deve ser usado/criado o login "Agilent\ECMServer \$" do Windows.)
- 4 Mapeie o usuário do Shared Services com o login do MS SQL Server.
 - a Selecione **Mapa** para o banco de dados OLSharedServices.
 - b Mapeie o login do MS SQL para o usuário do banco de dados do Shared Services da Etapa 1.
 - c Mapeie o Esquema Padrão dbo para o usuário OLSS.

Definir as configurações do banco de dados datarepo usando o SQL Management Studio

- 1 Verifique o usuário do banco de dados em **datarepo > Segurança > Usuários** (revise os usuários para reutilizar o usuário existente. Caso o banco de dados tenha sido restaurado para um novo servidor, remova e crie um novo.).
- 2 Verifique os logins do MS SQL Server.
 - a Acesse **Segurança > Logins**.
 - b Caso o banco de dados tenha sido restaurado para um novo servidor, remova o usuário do banco de dados e crie um novo.
 - Autenticação no servidor SQL.
 - A senha não expira. Use a mesma senha usada antes da restauração.
 - Mapeie o novo usuário para o banco de dados **OLSharedServices**.
- 3 Verifique as propriedades do usuário do banco de dados em Banco de dados do **Shared Services > Segurança > Usuários** e modifique a participação do usuário para a função **db_owner**.

Etapas 4 Restaurar conteúdo

Determine os locais da pasta de conteúdo do OpenLab Sever/ECM XT (**C:\SSStorage**) e restaure-a a partir do seu backup. É recomendado usar os caminhos originais para simplificar configurações posteriores.

Se você tiver múltiplos locais de armazenamento de conteúdo, cada local de armazenamento de conteúdo adicional deve ser restaurado para seu próprio local.

Para topologias nas quais os armazenamentos estão localizados em recursos de rede compartilhados, o usuário, após restaurar os armazenamentos, também precisará restaurar as permissões ou cuidar de sua disponibilidade para o servidor.

Etapas 5 Restaurar as informações de configuração do OpenLab Server/ECM XT

Restaure o conteúdo das seguintes pastas a partir do backup:

```
%ProgramData%\Agilent\Installation
%ProgramData%\Agilent\OpenLab Certificate Service
%ProgramData%\Agilent\OpenLab Platform\OpenSearch
%ProgramData%\Agilent\OpenLab Platform\Reverse Proxy
```

Abaixo estão comandos de exemplo, que podem ser executados usando uma janela CMD do Windows ou um arquivo em lote. Os comandos têm de ser alterados para corresponder ao local de backup escolhido. Certifique-se de executar os comandos em uma janela CMD com privilégios de Administrador. Ao copiar/colar, remova o CRLF das linhas.


```

REM Comandos para um arquivo em lote do Windows para restaurar manualmente
arquivos de configuração, BD e dados de gestão de conteúdo
REM Precisa ser executado como Administrador
REM Nos exemplos abaixo, todos os dados são restaurados de pastas na unidade E:
REM
REM Certifique-se de que a pasta para o arquivo de registro existe (p. ex.:
C:\temp)
REM Restaure os arquivos de instalação e configuração do OpenLab
robocopy "E:\ProgramData\Installation" "%ProgramData%\Agilent\Installation" /e
/zb /purge /IS /IT /IM /log:C:\temp\olrestore.log
REM Comente ou remova a próxima linha, se os arquivos forem restaurados em um
servidor com um nome de host diferente. Neste caso, os certificados não serão
restaurados
robocopy "E:\ProgramData\OpenLab Certificate Service"
"%ProgramData%\Agilent\OpenLab Certificate Service" /e /zb /purge /IS /IT /IM
/log+:C:\temp\olrestore.log
REM
robocopy "E:\ProgramData\Reverse Proxy" "%ProgramData%\Agilent\OpenLab
Platform\Reverse Proxy" /e /zb /purge /IS /IT /IM /log+:C:\temp\olrestore.log
REM
REM Copie os arquivos do BD PostgreSQL - requer o encerramento prévio do
serviço do banco de dados
robocopy "E:\ProgramData\PostgreSQL" "%ProgramData%\Agilent\OpenLab
Platform\PostgreSQL" /e /zb /purge /IS /IT /IM /log+:C:\temp\olrestore.log
REM
REM
REM Copie o armazenamento de conteúdo da gestão de conteúdo eletrônico
(em vários threads para um backup mais rápido)
robocopy "E:\SStorage" "C:\SStorage" /e /zb /mt:4 /purge /IS /IT /IM
/log+:C:\temp\olrestore.log

```

Revise o arquivo de registro quanto a divergências ou arquivos ignorados ou com falhas.

Etapas 6 Restaurar a infraestrutura de certificados

- 1 Verifique se o Agilent OpenLab Certificate Service está parado.
- 2 Vá para C:\ProgramData\Agilent\OpenLab Certificate Service\v1\hosts. Nesta fase, o servidor de hosts deverá mostrar uma pasta com o nome do servidor antigo.
- 3 Inicie o Agilent OpenLab Certificate Service. A pasta c:\ProgramData\Agilent\OpenLab Certificate Service\v1\hosts deverá mostrar uma nova pasta com o nome do novo servidor.
- 4 Teste o certificado do novo servidor acessando <https://localhost:52088/openlab/certservice/info>. A conexão deverá ser reportada como segura.
- 5 Reinicie o serviço Agilent OpenLab Reverse Proxy.
- 6 Teste a vinculação do novo certificado ao proxy reverso acessando <https://localhost/openlab/certservice/info>. A conexão deverá ser reportada como segura.

Etapas 7 Reiniciar

Reinicie a máquina e faça login como administrador.

Etapas 8 Alterar o servidor de licenças no OpenLab Control Panel

Siga este procedimento se o servidor de licença for movido para um computador com um nome diferente.

- 1 Faça login no OpenLab Control Panel como administrador. Em caso de falha de conexão, certifique-se de que todos os serviços do SDMS e do Shared Services tenham sido iniciados após a reinicialização.
- 2 Clique em **Administração > Licenças > Alterar Servidor**.
- 3 Digite o nome do servidor da licença.
- 4 Clique em **Ping** para verificar se o novo servidor está correto.
- 5 Clique em **OK**.
- 6 Reinicie a máquina.

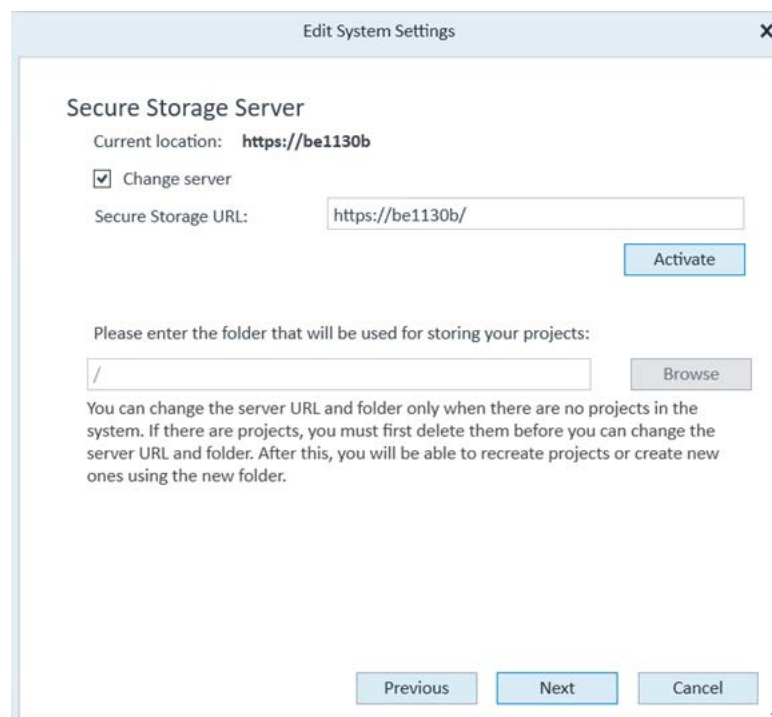
Etapa 9 Executar o utilitário de configuração

- 1 Execute o Utilitário de Configuração em **Iniciar > Agilent Technologies > Utilitário de Configuração**.
- 2 No Control Panel para OpenLab, verifique se as guias **Projetos** e **Instrumentos** agora estão visíveis.

Etapa 10 Ativar o OpenLab Server/ECM XT

Se a Restauração estiver sendo realizada com o mesmo nome de host, o OpenLab Server/ECM XT não precisará ser reativado. No entanto, se o servidor for movido para uma nova máquina, o OpenLab Server/ECM XT exigirá uma reativação.

- 1 Abra a guia **OpenLab Control Panel > Administração**.
- 2 Clique em **Configuração do Sistema > Editar Configurações do Sistema**.
- 3 Selecione **Manter a configuração atual**.
- 4 Selecione **Secure Storage** como tipo de armazenamento e clique em **Próximo**.
- 5 Clique em **Próximo**.
- 6 Selecione **Alterar o servidor**, digite a URL do OpenLab Server/ECM XT e clique em **Ativar** para reativar a sincronização do OpenLab Server/ECM XT.



7 Clique em **Próximo** e, em seguida, clique em **Aplicar**.

NOTA

Se você estiver usando o Sample Scheduler, os serviços do Sample Scheduler deverão ser reiniciados após o procedimento de restauração.

Etapa 11 Verificar os locais de armazenamento e a indexação do registro de atividades

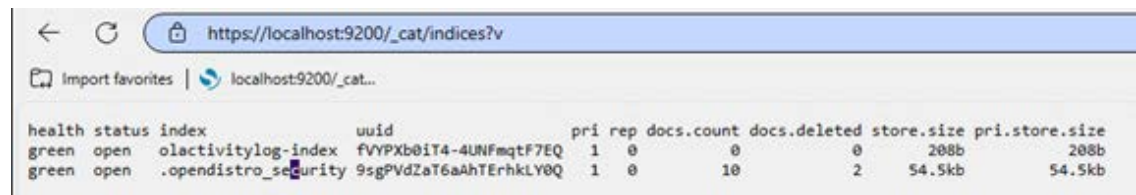
1 Abra um navegador da Web, insira o URL: <https://localhost/openlab-storage-admin/> e faça login com uma conta administrativa.

Uma página da Web é exibida e fornece os caminhos para os locais de armazenamento de gestão de conteúdo. Verifique se a lista corresponde aos locais de armazenamento restaurados.

2 Abra um navegador da Web, insira o URL: https://localhost:9200/_cat/indices?v e faça login como usuário dradmin. A lista de índices deverá mostrar o índice-olactivitylog com o status de integridade verde.

NOTA

A recriação do índice de registro de atividades poderá precisar de várias horas. Durante esse período, o Registro de atividades não pode ser pesquisado no OpenLab Control Panel.



health	status	index	uuid	pri	rep	docs.count	docs.deleted	store.size	pri.store.size
green	open	olactivitylog-index	fVYPXb0iT4-4UNFmqTF7EQ	1	0	0	0	208b	208b
green	open	.opendistro_security	9sgPVdZaT6aAhTErhkLY0Q	1	0	10	2	54.5kb	54.5kb

Caso o registro de atividades não apareça no Control Panel, recrie o índice:

- Execução inicial:
 - Esse comando recria o índice OpenSearch excluindo o índice atual e indexando todo o banco de dados ActivityLog no OpenSearch.
 - Essa linha de comando deve ser usada como a primeira execução do ALBIT após a restauração de um banco de dados.

Uma mensagem de confirmação será exibida no console para garantir que você deseja continuar.

```
Agilent.OpenLab.ActivityLog.Tools.Albit.exe rebuild-index
```

 - Para ignorar a mensagem de confirmação (em um ambiente não interativo), passe a opção `--force`.

```
Agilent.OpenLab.ActivityLog.Tools.Albit.exe rebuild-index --force
```
- Continuação após tempo limite na execução anterior:
 - Se a última execução do ALBIT atingiu o tempo limite durante a indexação em massa, deve ser executada com a opção `--continue`.

Isso não excluirá o índice OpenSearch atual nem o progresso de indexação atual, mas continuará de onde a última execução parou.

Isso evita a necessidade de iniciar todo o processo novamente devido a um tempo limite atingido.

```
Agilent.OpenLab.ActivityLog.Tools.Albit.exe rebuild-index --continue
```

Etapa 12 Configuração de cliente

Se o servidor OpenLab Server/ECM XT tiver sido restaurado para um host diferente, cada controlador de instrumentos da Agilent ou cliente na configuração deverá ser configurado para o novo servidor OpenLab Server/ECM XT. Esse procedimento deve ser repetido em cada máquina-cliente.

- 1 Selecione **Iniciar > Todos os programas > Agilent Technologies > Shared Services Maintenance**.
- 2 Clique na guia **Parâmetros do Servidor**.
- 3 Clique em **Adicionar Servidor** e forneça um Nome e uma Descrição opcional.
- 4 Insira o nome do host novo no campo **Servidor** e clique em **Testar Conexão**.
- 5 Clique em **OK** e configure este servidor como padrão. Agora é possível iniciar sessão no Control Panel.

Etapa 13 Atualizar marcações do Navegador de Conteúdo

Se os navegadores da Web do PC cliente contêm marcações de Navegador de Conteúdo, atualize as marcações usando o nome do novo servidor. Por exemplo: <https://<new OpenLab Server>/openlab-storage/>

Etapa 14 Verificar a licença no Control Panel

Se o seu endereço MAC do servidor mudar durante uma atualização do servidor, a licença para o novo servidor será diferente da licença do servidor antigo.

- 1 No **Control Panel**, selecione **Administração > Licenças**.
- 2 Na barra de ferramentas **Licenciamento**, clique em **Visualizar Licenças**. As informações serão exibidas em uma janela da Internet.

Reaplique a licença, se necessário. Consulte a Ajuda do Control Panel para obter mais informações.

Considerações sobre Hot Backup Manual

Diretrizes de Backup 77

Visão Geral 78

Backup Manual do Banco de Dados 79

Fazer backup dos bancos de dados 80

Backup Manual do Content Store 81

Backup Manual da Configuração do Servidor OpenLab Server/ECM XT 82

Armazenar os Arquivos de Backup 83

Restauração do Sistema 84

Este capítulo é destinado aos administradores com experiência em backup e manutenção de banco de dados e do Windows Server. As instruções incluem as informações necessárias para executar um hot backup do sistema OpenLab Server/ECM XT, incluindo o hot backup de banco de dados, armazenamento de conteúdo e informações de configuração.

NOTA

Os Utilitários de Backup e Restauração fornecem hot backup para os sistemas suportados. A Agilent recomenda o uso de Utilitários de Backup e Restauração sempre que possível. Consulte "**Procedimentos de Backup e Restauração**" na página 41 para obter informações sobre como usar os Utilitários de Backup e Restauração.

NOTA

O backup do índice não é feito, mas ele é reconstruído após a restauração.

Diretrizes de Backup

- Siga sempre a ordem prescrita, conforme descrito em **"Visão Geral"** na página 78 ao fazer backup do sistema.
- Embora o hot backup tenha sido desenvolvido para ser executado enquanto os usuários estão ativos no sistema, há um impacto no desempenho . É preferível executá-lo durante períodos de menor atividade do sistema, por exemplo, quando o arquivamento não está sendo executado e a taxa de upload está em níveis normais ou abaixo do normal.

Visão Geral

Um hot backup permite que todos os dados comprometidos do OpenLab Server/ECM XT sejam copiados em um estado consistente enquanto o sistema continua funcionando. É importante executar o procedimento de backup na seguinte ordem.

- 1 Banco de dados** – Ao operar com o modelo de recuperação simples do Microsoft SQL Server ou usar o recurso de despejo de SQL do PostgreSQL, o backup do banco de dados deve ser concluído antes do backup do armazenamento de conteúdo. Isto garantirá a consistência dos registros comprometidos no banco de dados e no armazenamento de conteúdo.
- 2 Armazenamento de Conteúdo** – A próxima etapa é fazer backup dos arquivos reais. Para isso, utilize qualquer ferramenta de backup de arquivos.
- 3 Informações de Configuração** – A etapa final é fazer o backup do arquivo de configuração, o que simplificará a reinstalação do software. Para isso, utilize qualquer ferramenta de backup de arquivos.

NOTA

Após a conclusão dos backups, é importante que você armazene o banco de dados e o backup do armazenamento de conteúdo juntos como uma única unidade, pois eles devem ser restaurados como um conjunto, caso contrário, o sistema não funcionará corretamente.

NOTA

O backup do índice não é feito, mas ele é reconstruído após a restauração.

Backup Manual do Banco de Dados

Em um sistema OpenLab Server/ECM XT, a capacidade de suportar hot backups depende dos recursos de hot backup do banco de dados que o OpenLab Server/ECM XT está configurado para utilizar. Para fazer hot backups, o banco de dados utilizado deve ter uma ferramenta que possa capturar o "snapshot" de uma versão consistente do banco de dados OpenLab Server/ECM XT. (Ou seja, ele deverá capturar uma cópia de transação consistente de todas as tabelas no banco de dados OpenLab Server/ECM XT.) Além disso, para evitar problemas graves de desempenho no sistema OpenLab Server/ECM XT em execução enquanto o backup estiver em andamento, essa operação de "snapshot" deverá operar sem estabelecer bloqueios no banco de dados do OpenLab Server/ECM XT ou deverá ser concluída rapidamente (dentro de segundos).

Os recursos de backup variam entre o Microsoft SQL Server e o PostgreSQL. Certifique-se de que todos os procedimentos de backup sejam validados por um administrador de banco de dados qualificado e experiente antes de serem colocados em um ambiente de produção.

Para fazer backup do banco de dados, faça o seguinte:

- 1 Verifique se o banco de dados está instalado e configurado conforme mostrado no *Guia de Instalação Agilent OpenLab ECM Server e ECM XT*.
- 2 Para os bancos de dados hospedados no PostgreSQL, identifique os nomes do banco de dados do conteúdo e do banco de dados do Shared Services que foram especificados no momento da instalação. É possível determinar esses nomes da seguinte maneira:
 - a Execute o aplicativo Configuração do Servidor (**Iniciar > Agilent Technologies > Configuração do Servidor**). Isso fornece um resumo da configuração personalizada do Shared Services.
 - b No Resumo do Banco de Dados do Shared Services, você encontrará o Nome do Banco de Dados dos serviços compartilhados.

Tabela 6. Resumo do banco de dados do Shared Services

Tipo de banco de dados	PostgreSQL
Nome do servidor	localhost
Instância do servidor	Não aplicável
Porta do servidor	5432 (padrão)
Nome do banco de dados	OLSharedServices (padrão)
Administrador do banco de dados	postgres
Usuário do banco de dados	Olss (padrão)

- c O nome do banco de dados do conteúdo é mostrado na tabela a seguir.

Tabela 7. Resumo do banco de dados do Content Management

Tipo de banco de dados	PostgreSQL
Nome do servidor	localhost
Instância do servidor	Não aplicável
Porta do servidor	5432

Tabela 7. Resumo do banco de dados do Content Management

Nome do banco de dados	datarepo
Administrador do banco de dados	postgres
Usuário do banco de dados	DSAdmin

- 3 Com os nomes dos bancos de dados em mãos, utilize as instruções e a ferramenta de backup do banco de dados apropriadas para fazer backup de todas as tabelas.

Fazer backup dos bancos de dados

Criar e restaurar hot backups de um PostgreSQL ou Servidor SQL requer um administrador de banco de dados profissional. É recomendado usar os procedimentos e ferramentas fornecidos pelo fornecedor do software do banco de dados.

Considerações adicionais sobre backup

- Backup externo – Para obter mais proteção, copie os arquivos de backup para um local externo. No mínimo, os backups devem ser armazenados em um dispositivo separado dos arquivos do banco de dados do PostgreSQL ou do Servidor SQL.
- Para cada backup que você optar por manter, copie os arquivos de backup do banco de dados para um local separado, juntamente com os backups do arquivo de conteúdo, para que um conjunto correspondente seja mantido.
- Criptografia – Para proteger ainda mais os dados, considere criptografar os arquivos de backup.
- Agendar tarefas de backup do banco de dados – As tarefas de backup podem ser agendadas utilizando o Agendador do Windows, por exemplo.

Backup Manual do Content Store

Para fazer backup do armazenamento de conteúdo, utilize qualquer utilitário de backup de arquivo. É recomendável utilizar um que possa executar backups diferenciais. Dessa forma, não é necessário sempre fazer o backup de todo o armazenamento de conteúdo, basta fazer um backup incremental. É importante que você possa restaurar seus índices, banco de dados e armazenamento de conteúdo do arquivo para um estado consistente. Para fazer backup dos arquivos de conteúdo, será necessário identificar o local do armazenamento de conteúdo. Para encontrar o local do armazenamento de conteúdo, faça o seguinte:

- 1 Vá até a máquina do servidor OpenLab Server/ECM XT. Em um ambiente empresarial, é possível se conectar a qualquer nó.
- 2 Consulte a Etapa 1 em "**Procedimentos Manuais de Cold Backup e Restauração**" na página 62 para obter detalhes sobre como determinar o local dos armazenamentos de conteúdo.
- 3 Se o seu repositório tiver múltiplos armazenamentos de conteúdo, será necessário realizar o backup de cada um desses armazenamentos de conteúdo adicionais.
- 4 Depois de identificar todos os locais de armazenamento de conteúdo, utilize sua ferramenta de backup de arquivos para fazer backup deles.

Backup Manual da Configuração do Servidor OpenLab Server/ECM XT

Consulte os "**Procedimentos Manuais de Cold Backup e Restauração**" na página 62 para obter detalhes sobre como fazer backup das informações de configuração do OpenLab Server. Como estas informações são estáticas, elas não precisam fazer parte de todo procedimento de hot backup agendado. Pelo menos um cold backup completo é recomendado.

Armazenar os Arquivos de Backup

Para garantir que você tenha um conjunto consistente de banco de dados e conteúdo, é necessário implementar um processo para salvar o resultado dessas etapas de backup diariamente e organizá-las para que o conjunto correspondente possa ser encontrado caso o sistema precise ser restaurado. Também é possível optar por armazenar os arquivos do mesmo conjunto juntos ou apenas documentar as etapas para encontrar o conjunto, tendo em mente que a ordem necessária para realizar os backups é:

- 1 Bancos de dados
- 2 Armazenamento(s) de conteúdo
- 3 Informações de Configuração

Restauração do Sistema

Configure um sistema consistente com a configuração em utilização no momento do backup. Isso pode ser feito manualmente, seguindo as mesmas etapas de instalação e configuração efetuadas originalmente, juntamente com as etapas subsequentes feitas ao longo do tempo. Outra abordagem pode ser incluir um backup completo do sistema como base e atualizá-lo conforme você atualiza a configuração. Você é responsável por decidir como configurar seu plano de recuperação de desastres. No entanto, será necessário começar com a configuração correta para restaurar seu conjunto de dados e ter um sistema em execução.

Para restaurar os dados, comece com um sistema em funcionamento, encerre os serviços, o banco de dados, o Data Repository, o armazenamento de conteúdo e o arquivo de Configuração do Servidor. A ordem de restauração não é relevante. O importante é que você restaure um conjunto de dados consistente e completo. Para fazer isso, considere o seguinte:

- Não deixe nenhum dado existente no banco de dados. Comece com um banco de dados vazio.
 - Verifique se os armazenamentos de conteúdo estão vazios ao iniciar a restauração. Se você estiver utilizando vários armazenamentos de conteúdo, coloque o conjunto certo de arquivos em cada local.
- 1 Restaure o banco de dados.
 - 2 Restaure as pastas do armazenamento de conteúdo.
 - 3 Restaure os arquivos de configuração e o servidor de aplicativos conforme descrito em **"Procedimentos Manuais de Cold Backup e Restauração"** na página 62.
 - 4 Recrie o índice conforme descrito em **"Procedimentos Manuais de Cold Backup e Restauração"** na página 62.

Após restaurar todos os dados, reinicie o servidor.

Considerações sobre a Restauração

Caso seja necessário recuperar o sistema, recupere todos os tipos de dados (banco de dados, conteúdo e arquivos de configuração) do mesmo conjunto para garantir a consistência dos dados do sistema. Dependendo da falha do banco de dados que está obrigando a restauração do backup, as etapas necessárias poderão variar.

Mover o Servidor de Aplicativos OpenLab Server/ECM XT para um Novo Sistema Operacional 86

Reconfiguração do Servidor OpenLab Server/ECM XT 87

Desativar o OpenLab Server/ECM XT 87

Fazer alterações na infraestrutura 89

Executar o Utilitário de Configuração do OpenLab Server 92

Ativar o OpenLab Server/ECM XT 93

Acrescentar repositório de arquivo ou conteúdo adicional 93

Alterar a Senha do Shared Services 94

Mover o Servidor de Aplicativos OpenLab Server/ECM XT para um Novo Sistema Operacional

- 1 Instale o OpenLab Server/ECM XT na nova máquina com o novo sistema operacional.
- 2 Na máquina antiga, realize um backup manual do sistema. Consulte **"Backup do OpenLab Server/ECM XT Usando o Utilitário de Backup"** na página 47 ou **"Procedimento Manual de Backup do Servidor de Aplicativos OpenLab Server/ECM XT"** na página 63
- 3 Na nova máquina, realize o procedimento de restauração do servidor. Consulte **"Restaurar o OpenLab Server/ECM XT Usando o Utilitário de Restauração"** na página 57 ou **"Procedimento Manual de Restauração do Servidor de Aplicativos OpenLab Server/ECM XT"** na página 68.

Reconfiguração do Servidor OpenLab Server/ECM XT

Essa seção cobre os cenários comuns, como o que se segue:

- Você tem uma instalação do OpenLab Server/ECM XT com um servidor de banco de dados (local ou remoto) e decidiu atualizar o software do servidor de banco de dados para uma versão mais recente ou atualizar o hardware, o que envolve a recolocação do software do servidor de banco de dados em uma nova máquina. Você deverá indicar ao OpenLab Server/ECM XT como conectar ao novo servidor de banco de dados e continuar a trabalhar.
- Um servidor de arquivos não possui espaço livre, por isso você decide mover o armazenamento do conteúdo para outro hardware.
- Uma alteração na política de segurança corporativa tornou necessária a alteração dos usuários do sistema e das senhas utilizadas pelo OpenLab Server/ECM XT.

As páginas a seguir descrevem como realizar essas tarefas.

Em geral, o processo consiste em quatro etapas:

- 1 **"Desativar o OpenLab Server/ECM XT"** na página 87
- 2 **"Fazer alterações na infraestrutura"** na página 89
- 3 **"Executar o Utilitário de Configuração do OpenLab Server"** na página 92
- 4 **"Ativar o OpenLab Server/ECM XT"** na página 93

Para acrescentar armazenamento de conteúdo ou arquivo adicional, consulte **"Acrescentar repositório de arquivo ou conteúdo adicional"** na página 93.

Desativar o OpenLab Server/ECM XT

- 1 Abra os Serviços do Windows (services.msc) e pare o serviço: Serviço de Download e Upload do Agilent OpenLab SDMS.
- 2 Abra um navegador da Web e acesse o URL:
<https://localhost:15671/openlab/rabbitmq/#/queues>
- 3 Faça login na fila de mensagens RabbitMQ como o usuário dradmin.
- 4 Na guia Filas, verifique se todas as filas estão ociosas e se não existem entradas pendentes.
- 5 prossiga com a interrupção dos serviços:
 - Agilent OpenLab Shared Services
 - Serviço de certificados
 - Todos os serviços do SDMS OpenLab
 - Todos os serviços relacionados ao repositório de dados
 - OpenSearch 2.5.0 (opensearch-service-x64)
 - PostgreSQL 15.1.1.80 (x64) (somente aplicável ao usar o banco de dados PostgreSQL para o OpenLab Server/ECM XT). Ignore este serviço se o banco de dados estiver em um host separado.
 - RabbitMQ

Abaixo estão comandos de exemplo que podem ser executados usando uma janela de comando do Windows (com privilégios de administrador) ou um arquivo em lote. Estes comandos interromperão todos os serviços relevantes do OpenLab.

REM Estes comandos interrompem todos os serviços relevantes do OpenLab CDS para que um cold backup possa ser realizado

```
net stop "Agilent OpenLab Activity Log Service"
net stop "Agilent OpenLab Audit Trail Service"
net stop "AutomationServerHost"
net stop "Agilent OpenLab Backup Monitoring Service"
net stop "Agilent OpenLab Backup Notification Service"
net stop "Agilent OpenLab Backup Task Status Cache Service"
net stop "OpenLabCertificateService"
net stop "DataCollectionAgent"
net stop "DataCollectionService"
net stop "DataRepositoryBaseService"
net stop "Agilent OpenLab Distributed Transaction Coordinator Service"
net stop "Agilent OpenLab Electronic Signature Service"
net stop "Agilent OpenLab License Server"
net stop "Agilent OpenLab Licensing Support"
net stop "Agilent OpenLab CopyTo Server"
net stop "DiagnosticsToolsService"
net stop "AuthenticationService"
net stop "BrowsingService"
net stop "BulkImportService"
net stop "ContentBrowserService"
net stop "DeleteService"
net stop "UploadDownloadService"
net stop "Agilent OpenLab SDMS Action Service"
net stop "SDMS_MetadataExtractionService"
net stop "SDMS_MetadataPersistenceService"
net stop "SDMS_MetadataQueryService"
net stop "PermissionsSyncService"
net stop "SecureStorageAdministrationService"
net stop "StorageConfigurationService"
net stop "StorageManagementService"
net stop "SharedServicesHost"
net stop "Agilent.Scheduler.Webserver"
net stop "Agilent Sample Scheduler Database Management Agent"
net stop "Agilent Sample Scheduler Services Controller"
net stop "Agilent.Scheduler.Lims.Agent"
net stop "Agilent.Scheduler.Orchestrator"
net stop "Agilent.TestServices.WebService"
net stop "Agilent.TestServices.Server.Main"
net stop "OpenLabReverseProxy"
net stop "opensearch-service-x64"
net stop "RabbitMQ"
net stop "postgresql-x64-15-dr"
```


Fazer alterações na infraestrutura

Mover o servidor de BD

Mova os bancos de dados do OpenLab Server/ECM XT e do Shared Services para o novo servidor. Esta etapa é específica para o tipo de BD usado.

Mover um banco de dados do Servidor SQL Consulte a documentação do fornecedor para mover bancos de dados do Servidor SQL.

Mover um banco de dados PostgreSQL As versões do servidor do banco de dados de destino e de origem devem ser iguais. Os dígitos das versões principal e secundária devem ser iguais, por exemplo, 15.x.x.x. Para este exemplo,

- Servidor1 é a máquina de origem
 - Servidor2 é a máquina de destino
- 1 No Servidor1, pare o serviço PostgreSQL (para a versão 15: **postgresql 15.x.x.x (x64)**).
 - 2 No Servidor 1, localize a pasta do banco de dados PostgreSQL e faça backup dessa pasta. (Por exemplo, C:\ProgramData\Agilent\OpenLab Platform\PostgreSQL\15.) Para obter instruções sobre como fazer backup do banco de dados, consulte ["Fazer um backup manual do sistema"](#) na página 63.
 - 3 No Servidor2, descompacte a pasta do banco de dados PostgreSQL. Atribua o nome **PG_DATA_NEW**.
 - 4 Execute do instalador PostgreSQL. Se for solicitada a pasta de dados, insira **PG_DATA_NEW**.
 - 5 Clique em **Próximo** até a instalação estar concluída.
 - 6 Se, depois da reconfiguração, seu servidor PostgreSQL estiver em uma máquina diferente da instalação do OpenLab Server/ECM XT, siga estas etapas. Caso contrário, avance para a [etapa 7](#).

Para usar uma conexão remota ao PostgreSQL usando a Autenticação do Windows:

- a Certifique-se de que o Servidor1, Servidor2 e o seu servidor OpenLab Server/ECM XT estejam todos conectados ao mesmo domínio.
- b Abra **pg_hba.conf** na pasta **PG_DATA_NEW** e certifique-se de que contenha as seguintes linhas:

```
host all "postgres" 172.16.0.111/32 md5
host all "postgres" ::1/128 md5
host all "SYSTEM" 127.0.0.1/32 sspi
host all "SYSTEM" ::1/128 sspi
host all all 127.0.0.1/32 md5
host all all ::1/128 md5
```

Adicione as seguintes linhas para um servidor OpenLab Server/ECM XT com endereço IPv4 172.16.0.111 e endereço IPv6 fc00:1ac4:65fb:34cb:e71c:db64:c33:e1ed:

```
host all "postgres" 172.16.0.111/32 md5
host all "postgres" fc00:1ac4:65fb:34cb:e71c:db64:c33:e1ed/128 md5
host all all 172.16.0.111/32 md5
host all all fc00:1ac4:65fb:34cb:e71c:db64:c33:e1ed/128 md5
```

Para obter mais informações sobre como configurar um servidor PostgreSQL externo, consulte a seção *Configurar um servidor de banco de dados PostgreSQL remoto* no *Guia de Instalação do Agilent OpenLab Server e OpenLab ECM XT*. Consulte o seu administrador de rede para encontrar a melhor opção para a sua rede.

- c Abra **pg_ident.conf** na pasta **PG_DATA_NEW** e adicione as seguintes linhas:

```
# MAPNAME    SYSTEM-USERNAME    PG-USERNAME
SecureStorage1 Server1$          SYSTEM
```

em que **Server1\$** é o nome do usuário do sistema remoto atribuído pelo PostgreSQL. Geralmente, o nome do usuário do sistema corresponde ao nome NetBIOS da máquina em que o OpenLab Server/ECM XT está sendo executado, seguido por um cifrão (\$).

Se ele não corresponder e se a Configuração do OpenLab ECM XT falhar, revise as últimas mensagens na pasta **PG_DATA_NEW > pg_log** para encontrar algo semelhante a:

```
2015-06-02 10:05:34 PDT FATAL: SSPI authentication failed for user
"SYSTEM"
```

```
2015-06-02 10:05:37 PDT LOG: provided user name (SYSTEM) and authenticated
user name (WIN-ITGSOV7UQM2$) do not match
```

em que WIN-ITGSOV7UQM2\$ é o SYSTEM_USERNAME que você deve colocar em **pg_ident.conf**.

Consulte a documentação oficial do PostgreSQL para saber mais sobre os recursos de segurança.

Para usar uma conexão remota ao PostgreSQL usando a autenticação SQL:

Abra **pg_hba.conf** na pasta **PG_DATA_NEW** e verifique se contém as seguintes linhas para um servidor OpenLab Server/ECM XT com endereço IPv4 172.16.0.111 abd endereço IPv6 fc00:1ac4:65fb:34cb:e71c:db64:c33:e1ed:

```
host all "postgres" 172.16.0.111/32 md5
host all "postgres" fc00:1ac4:65fb:34cb:e71c:db64:c33:e1ed/128 md5
host all all 172.16.0.111/32 md5
host all all fc00:1ac4:65fb:34cb:e71c:db64:c33:e1ed/128 md5
```

É possível definir intervalos de sub-rede em vez de endereços IP únicos em pg_hba.conf. O exemplo a seguir permite todas as conexões com o servidor de banco de dados PostgreSQL originadas do intervalo de endereços 172.16.0.0 a 172.16.0.255 e do intervalo de endereços IPv6 fc00:1ac4:65fb:34cb::/64:

```
host all "postgres" 172.16.0.0/24 md5
host all "postgres" fc00:1ac4:65fb:34cb::/64 md5 0.0/24 md5
host all all fc00:1ac4:65fb:34cb::/64 md5
```

Consulte a documentação oficial do PostgreSQL para saber mais sobre os recursos de segurança.

- 7 Para aplicar as alterações, reinicie o serviço PostgreSQL.

Alterar o local de armazenamento do conteúdo seguro

Os caminhos para os locais de armazenamento não podem ser modificados após a criação e os locais de armazenamento existentes não podem ser excluídos. Se a modificação ou exclusão de um local de armazenamento existente for necessária, entre em contato com o Suporte da Agilent para obter ajuda.

Ao mover um servidor com armazenamento de arquivo local para um novo servidor, os arquivos devem ser restaurados para o mesmo caminho no novo servidor em que estavam originalmente localizados. Por exemplo, se o local de armazenamento estava originalmente em C:\SSStorage\Storage no servidor original, os arquivos devem ser restaurados para o mesmo caminho no novo servidor.

O aplicativo da Web Administração de Armazenamento oferece ferramentas para gerenciar onde o conteúdo físico é armazenado. Este aplicativo permite que um administrador realize as seguintes tarefas.

- Criar um novo local de armazenamento.
- Alterar qual local de armazenamento será usado para armazenar novos arquivos (Armazenamento Principal).
- Realocar arquivos de pastas de conteúdo específicas para um local específico de armazenamento.

Alterar usuários ou senhas do OpenLab ECM XT

É possível alterar a senha de usuários do banco de dados ou criar usuários e configurá-los para serem utilizados no OpenLab Server/ECM XT.

Se apenas desejar alterar a senha de um usuário do banco de dados existente, use um ambiente de desenvolvimento integrado (IDE) do banco de dados, como MS SQL Server Management Studio, pgAdmin IV etc., usando o procedimento padrão do software. Consulte a documentação oficial para obter detalhes.

Criar um novo usuário

- 1 Crie o usuário.
- 2 Conceda as permissões de usuário nas tabelas do banco de dados.

Por exemplo, se você criou um usuário de "teste" para o Banco de Dados Shared Services, execute o seguinte script para conceder privilégios em todas as tabelas do banco de dados.

```
DO
$$
DECLARE
    r information_schema.tables%rowtype;
    user_name VARCHAR = 'test'; -- specify username
BEGIN
    FOR r IN SELECT * FROM information schema.tables WHERE tab schema='public'
    LOOP
        RAISE NOTICE 'EXECUTE "ALTER TABLE % OWNER TO %";"', r.table_name, user_name;
        -- for debug
        EXECUTE 'ALTER TABLE ' || quote_ident(r.table_name) || ' OWNER TO ' ||
        user_name || ';' ;
    END LOOP;
END
$;
```

Para criar um novo usuário para um banco de dados do MS SQL Server Especifique o mapeamento de login do banco de dados usando o MS SQL Server Management Studio. Certifique-se de que o usuário é um membro das funções de banco de dados **db_datareader** e **db_datawriter** para as tabelas desejadas.

Você deve executar consultas com as credenciais de Administrador do Banco de Dados.

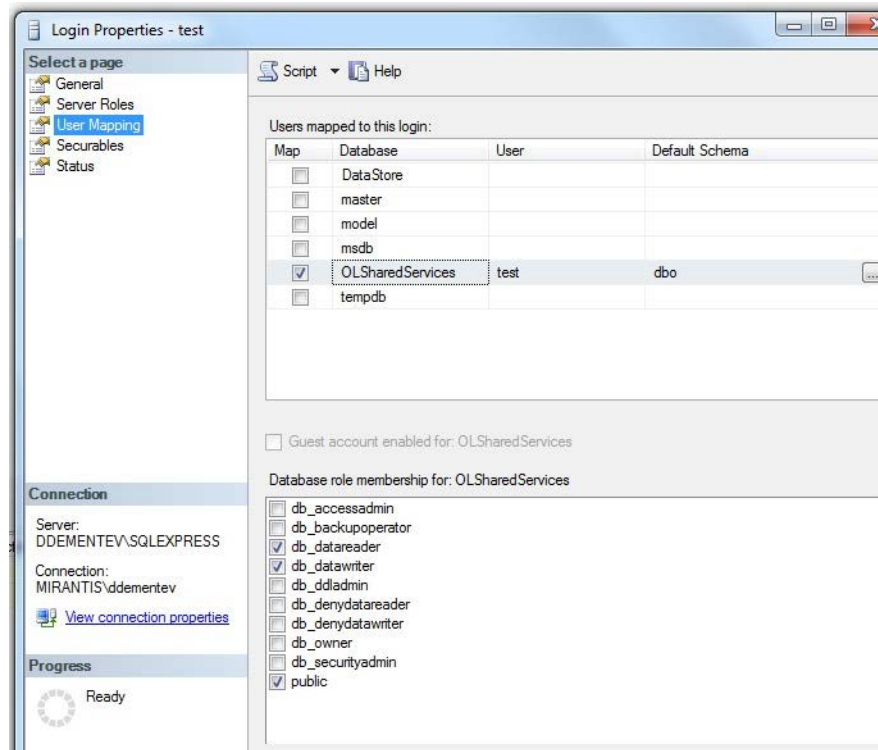


Figura 2. MS SQL Server Management Studio

Executar o Utilitário de Configuração do OpenLab Server

O Utilitário de Configuração do Servidor do OpenLab é instalado no servidor e pode ser executado de forma independente sem o instalador. O Utilitário de Configuração está listado no menu de inicialização do Agilent Technologies.

CUIDADO

Cada tela no Utilitário de Configuração do OpenLab Server está pré-preenchida com padrões que refletem a configuração real do OpenLab Server/ECM XT. Edite somente os campos que refletem alterações feitas em "**Fazer alterações na infraestrutura**" na página 89. É altamente recomendado que você não edite outros valores. A alteração de outros campos poderá causar a falha da configuração.

- 1 Na mídia de instalação do OpenLab Server/ECM XT, execute o Instalador do OpenLab (setup.exe).
- 2 Selecione **OpenLab Server/ECM XT > Padrão** e clique em **OK**.
- 3 No Instalador do OpenLab, clique em **Instalação do Servidor > Etapa 4 – Configurar ou reconfigurar o OpenLab Server/ECM XT**.
- 4 Na tela de Boas-vindas, clique em **Próximo**.

- 5 Na página Credenciais de Acesso, insira suas credenciais de acesso à conta. Ou insira um novo nome de usuário e senha para acessar o local do conteúdo. Clique em **Próximo**.
- 6 A seção Local de Armazenamento é ignorada durante a reconfiguração. Todas as alterações no armazenamento são realizadas usando o aplicativo da Web Administração de Armazenamento.
- 7 Por padrão, é instalado um certificado interno do Agilent OpenLab. Caso contrário, selecione **Usar um certificado personalizado existente** e insira as informações do certificado. Em seguida, clique em **Próximo**.

NOTA

Não selecione **Atualizar o certificado interno** porque o nome do host da máquina mudou. Se o nome do host tiver mudado, entre em contato com o Suporte da Agilent.

- 8 Revise o resumo de configuração atualizado e clique em **Aplicar**.
- 9 Após a conclusão da configuração, clique em **Concluído**.

Ativar o OpenLab Server/ECM XT

Quando o processo estiver concluído, o OpenLab Server/ECM XT estará funcionando.

Para verificar se a nova configuração foi adquirida com sucesso,

- 1 Faça login no Control Panel para OpenLab e clique em **Administração > Secure Storage > Sincronizar Tudo**.
- 2 Faça login no Navegador de Conteúdo e certifique-se de que todo o conteúdo esteja no devido lugar.

Acrescentar repositório de arquivo ou conteúdo adicional

Os locais de repositório de arquivo ou conteúdo adicional são adicionados usando o cliente Web Administração de Armazenamento no seguinte URL: <https://<OpenLab application server name>/openlab-storage-admin/>. Para obter informações adicionais, consulte "[Administração de Armazenamento](#)" na página 10.

Alterar a Senha do Shared Services

Use o seguinte procedimento para alterar a senha do Shared Services (OLSS).

- 1 Usando um editor de texto, abra o arquivo configuration.xml localizado na pasta %ProgramData%\Agilent\Installation.
- 2 Na seção <SharedServices>, localize as linhas para <UserName> e <ObfuscatedPassword> mostradas no exemplo a seguir:

```
<UserName>Olss</UserName>  
<ObfuscatedPassword>FGz0uxm64MX1vw9iqkdbCeMG2VfTb77DNfDJE44FtxQ=</ObfuscatedPassword>
```

- 3 Insira a nova senha usando a sintaxe "plain-password:<new password>". Veja o exemplo a seguir como uma diretriz:

Para alterar a senha para "Admin123", altere o Elemento XML que a contém, como se segue:

```
<ObfuscatedPassword>plain-password:Admin123</ObfuscatedPassword>
```

- 4 Salve o arquivo.
- 5 Execute **Iniciar > Agilent Technologies > Utilitário de Configuração** e aceite os valores-padrão. O arquivo configuration.xml será atualizado com uma versão ofuscada da nova senha.

Assistência de Vendas e Suporte	96
---------------------------------	----

Assistência de Vendas e Suporte

Acesse o site a seguir para obter o contato do departamento de vendas e suporte local:

<https://www.agilent.com/en/support>

www.agilent.com

© Agilent Technologies, Inc. 2024

Nº doc. D0035354pt Rev. B.00

EDIÇÃO 05/2024

