



Guia de portabilidade

# FreeRTOS



# FreeRTOS: Guia de portabilidade

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

As marcas comerciais e imagens comerciais da Amazon não podem ser usadas no contexto de nenhum produto ou serviço que não seja da Amazon, nem de qualquer maneira que possa gerar confusão entre clientes ou que deprecie ou desprestigie a Amazon. Todas as outras marcas comerciais que não pertencem à Amazon pertencem a seus respectivos proprietários, que podem ou não ser afiliados, conectados ou patrocinados pela Amazon.

---

# Table of Contents

Portabilidade do FreeRTOS .....	1
O que é o FreeRTOS? .....	1
Portabilidade do FreeRTOS+TCP .....	1
Perguntas frequentes sobre portabilidade .....	1
Fazer download do FreeRTOS para portabilidade .....	3
Configuração do seu espaço de trabalho e projeto para portabilidade .....	4
Portabilidade da bibliotecas do FreeRTOS .....	5
Fluxograma de transferência .....	5
Kernel do FreeRTOS .....	7
Pré-requisitos .....	7
Configuração do kernel do FreeRTOS .....	7
Testes .....	8
Implementando as macros de registro em log da biblioteca .....	8
Testes .....	8
TCP/IP .....	9
Portabilidade do FreeRTOS+TCP .....	9
Testes .....	10
corePKCS11 .....	11
Quando implementar um módulo PKCS #11 completo .....	11
Quando usar a corePKCS11 do FreeRTOS .....	12
Portabilidade da corePKCS11 .....	12
Testes .....	13
Network Transport Interface .....	18
TLS .....	18
NTIL .....	18
Pré-requisitos .....	19
Portabilidade .....	19
Testes .....	20
coreMQTT .....	22
Pré-requisitos .....	22
Testes .....	22
Criação de demonstração de referência do MQTT .....	22
coreHTTP .....	24
Testes .....	24

Atualizações de OTA (Over-the-Air) .....	24
Pré-requisitos .....	25
Portabilidade de plataforma .....	25
Testes E2E e PAL .....	27
Bootloader de dispositivo de IoT .....	34
Cellular Interface .....	38
Pré-requisitos .....	38
Migração do MQTT versão 3 para o coreMQTT .....	40
Como migrar da versão 1 para a versão 3 para os aplicativos OTA .....	41
Resumo das alterações da API .....	41
Descrição das alterações necessárias .....	46
OTA_Init .....	46
OTA_Shutdown .....	50
OTA_GetState .....	51
OTA_GetStatistics .....	52
OTA_ActivateNewImage .....	52
OTA_SetImageState .....	53
OTA_GetImageState .....	54
OTA_Suspend .....	54
OTA_Resume .....	55
OTA_CheckForUpdate .....	55
OTA_EventProcessingTask .....	56
OTA_SignalEvent .....	57
Como integrar a biblioteca OTA como um submódulo em sua aplicação .....	58
Referências .....	58
Migrando da versão 1 para a versão 3 para a porta OTA PAL .....	59
Alterações em OTA PAL .....	59
Funções .....	59
Tipos de dados .....	61
Alterações de configuração .....	62
Alterações nos testes OTA PAL .....	64
Lista de verificação .....	64
Histórico do documentos .....	66
.....	lxxvii

# Portabilidade do FreeRTOS

## O que é o FreeRTOS?

Desenvolvido em parceria com as principais empresas de chips do mundo ao longo de um período de 20 anos, e agora baixado a cada 170 segundos, o FreeRTOS é um sistema operacional em tempo real (RTOS) líder de mercado para microcontroladores e microprocessadores pequenos. Distribuído livremente sob a licença de código aberto do MIT, o FreeRTOS inclui um kernel e um conjunto crescente de bibliotecas adequadas para uso em todos os setores. O FreeRTOS foi desenvolvido com ênfase na confiabilidade e facilidade de uso. O FreeRTOS inclui bibliotecas para conectividade, segurança e atualizações sem fios, e aplicativos de demonstração que mostram atributos do FreeRTOS em [placas qualificadas](#).

Para obter mais informações, visite [FreeRTOS.org](http://FreeRTOS.org).

## Portabilidade do FreeRTOS para sua placa do IoT

Será necessário fazer a portabilidade das bibliotecas de software do FreeRTOS para sua placa baseada em microcontrolador com base em seus atributos e em seu aplicativo.

Como fazer a portabilidade do FreeRTOS para seu dispositivo

1. Siga as instruções em [Fazer download do FreeRTOS para portabilidade](#) para fazer download da versão mais recente do FreeRTOS para portabilidade.
2. Siga as instruções em [Configuração do seu espaço de trabalho e projeto para portabilidade](#) para configurar os arquivos e as pastas no download do FreeRTOS para portabilidade e teste.
3. Siga as instruções em [Portabilidade da bibliotecas do FreeRTOS](#) para fazer a portabilidade das bibliotecas do FreeRTOS para o dispositivo. Cada tópico inclui instruções sobre como testar a portabilidade.

## Perguntas frequentes sobre portabilidade

O que é uma porta do FreeRTOS?

Uma porta do FreeRTOS é uma implementação específica da placa de APIs para as bibliotecas necessárias do FreeRTOS e o kernel do FreeRTOS ao qual sua plataforma oferece suporte. A

porta permite que as APIs funcionem na placa e implementa a integração necessária com os drivers de dispositivo e BSPs fornecidos pelo fornecedor da plataforma. A porta também deve incluir quaisquer ajustes de configuração (por exemplo, velocidade de clock, tamanho da pilha, tamanho do heap) exigidos pela placa.

Se você tiver dúvidas sobre a portabilidade que não foram respondidas nesta página ou no restante do Guia de Portabilidade do FreeRTOS, [consulte as opções de suporte do FreeRTOS disponíveis](#).

# Fazer download do FreeRTOS para portabilidade

Baixe a versão mais recente do FreeRTOS ou do Long Term Support (LTS) em [freertos.org](https://freertos.org) ou clone do GitHub ([FreeRTOS-LTS](#)) ou ([FreeRTOS](#)).

## Note

Recomendamos que você clone o repositório. A clonagem facilita o recebimento de atualizações para a ramificação principal à medida que elas são enviadas ao repositório.

Como alternativa, transforme as bibliotecas individuais em submódulos do repositório FreeRTOS ou FreeRTOS-LTS. No entanto, verifique se as versões da biblioteca correspondem à combinação listada no arquivo `manifest.yml` no repositório FreeRTOS ou FreeRTOS-LTS.

Depois de baixar ou clonar o FreeRTOS, você pode começar a fazer a portabilidade das bibliotecas do FreeRTOS para sua placa. Para obter instruções, consulte [Configuração do seu espaço de trabalho e projeto para portabilidade](#) e [Portabilidade da bibliotecas do FreeRTOS](#).

# Configuração do seu espaço de trabalho e projeto para portabilidade

Siga as etapas abaixo para configurar o espaço de trabalho e o projeto do:

- Use uma estrutura de projeto e crie um sistema que preferir para importar as bibliotecas do FreeRTOS.
- Crie um projeto usando um ambiente de desenvolvimento integrado (IDE) e uma cadeia de ferramentas compatíveis com sua placa.
- Inclua os pacotes de suporte da placa (BSP) e os drivers específicos da placa em seu projeto.

Depois que o espaço de trabalho estiver configurado, será possível começar a fazer a portabilidade de bibliotecas individuais do FreeRTOS.



# Portabilidade da bibliotecas do FreeRTOS

Antes de iniciar a portabilidade, siga as instruções em [Configuração do seu espaço de trabalho e projeto para portabilidade](#).

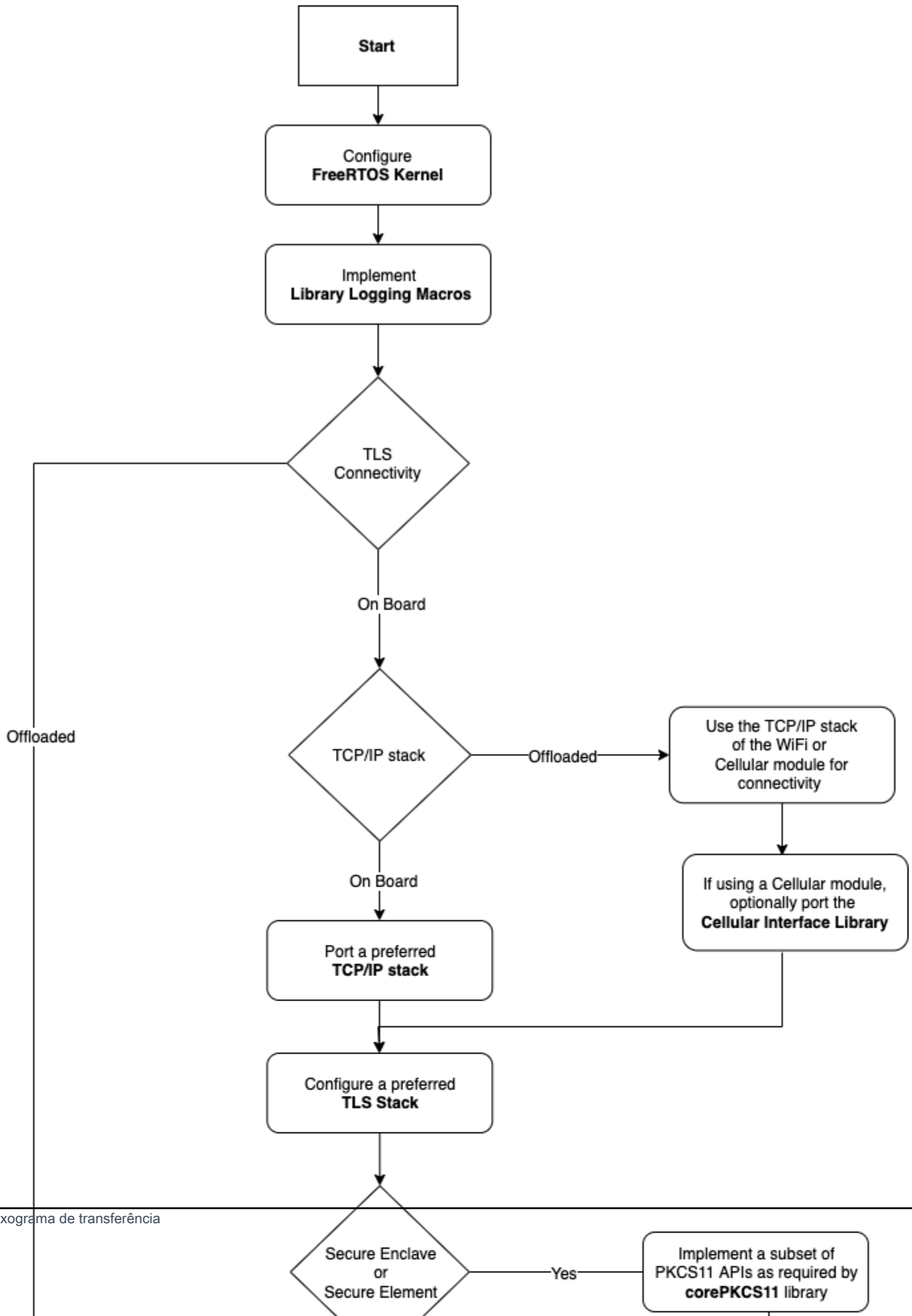
A [Fluxograma de portabilidade do FreeRTOS](#) descreve as bibliotecas necessárias para a portabilidade.

Para fazer a portabilidade do FreeRTOS para o dispositivo, siga as instruções nos tópicos a seguir.

1. [Configuração de uma porta do kernel do FreeRTOS](#)
2. [Implementando as macros de registro em log da biblioteca](#)
3. [Transferência de pilha de TCP/IP](#)
4. [Fazer portabilidade da Network Transport Interface](#)
5. [Portabilidade da biblioteca corePKCS11](#)
6. [Configuração da biblioteca coreMQTT](#)
7. [Configuração da biblioteca coreHTTP](#)
8. [Portabilidade da biblioteca de atualização sem fios do AWS IoT](#)
9. [Portabilidade da biblioteca Cellular Interface](#)

## Fluxograma de portabilidade do FreeRTOS

Use o fluxograma de portabilidade abaixo como auxílio visual ao fazer a portabilidade do FreeRTOS para sua placa.



# Configuração de uma porta do kernel do FreeRTOS

Esta seção fornece instruções para integrar uma porta do kernel do FreeRTOS em um projeto de teste de porta do FreeRTOS. Para obter uma lista de portas disponíveis do kernel, consulte [Portas do kernel do FreeRTOS](#).

O FreeRTOS usa o kernel do FreeRTOS para várias tarefas e comunicação entre tarefas. Para obter mais informações, consulte [Princípios básicos do kernel do FreeRTOS](#) no Guia do usuário do FreeRTOS e em [FreeRTOS.org](#).

## Note

A portabilidade do kernel do FreeRTOS para uma nova arquitetura não está incluída nessa documentação. Se você estiver interessado, [entre em contato com a equipe de engenharia do FreeRTOS](#).

Para o Programa de qualificação do FreeRTOS, apenas as portas existentes são compatíveis. Modificações nessas portas não são aceitas no programa. Revise a [política de portas do kernel do FreeRTOS](#) para obter mais informações.

## Pré-requisitos

Para configurar o kernel do FreeRTOS para portabilidade, é necessário o seguinte:

- Uma porta oficial do kernel do FreeRTOS ou portas com suporte para a plataforma de destino.
- Um projeto do IDE que inclui os arquivos de porta corretos do kernel do FreeRTOS para a plataforma e o compilador de destino. Para obter informações sobre a configuração de um projeto de teste, consulte [Configuração do seu espaço de trabalho e projeto para portabilidade](#).

## Configuração do kernel do FreeRTOS

O kernel do FreeRTOS é personalizado usando um arquivo de configuração chamado `FreeRTOSConfig.h`. Esse arquivo de cabeçalho especifica as definições de configuração específicas do aplicativo para o kernel. Para obter uma descrição de cada opção de configuração, consulte [Personalização](#) em FreeRTOS.org.

Para configurar o kernel do FreeRTOS para funcionar com seu dispositivo, inclua `FreeRTOSConfig.h` e modifique todas as configurações adicionais do FreeRTOS.

Para obter uma descrição de cada opção de configuração, consulte configurações de [personalização](#) em FreeRTOS.org.

## Testes

- Execute uma tarefa simples do FreeRTOS para registrar uma mensagem no console de saída serial.
- Verifique se a mensagem é enviada para o console conforme o esperado.

## Implementando as macros de registro em log da biblioteca

As bibliotecas do FreeRTOS usam as seguintes macros de registro em log, listadas em ordem crescente de detalhamento.

- `LogError`
- `LogWarn`
- `LogInfo`
- `LogDebug`

Uma definição para todas as macros deve ser fornecida. As recomendações são:

- As macros devem oferecer suporte ao registro em log de estilo C89.
- O registro em log deve ser seguro para thread. As linhas de log de várias tarefas não devem se intercalar umas com as outras.
- As APIs de registro em log não devem bloquear e devem liberar o bloqueio das tarefas do aplicativo na E/S.

Consulte a [funcionalidade de registro em log](#) em FreeRTOS.org para obter detalhes específicos de implementação. Você pode ver uma implementação neste [exemplo](#).

## Testes

- Execute um teste com várias tarefas para verificar se os registros não se intercalam.
- Execute um teste para verificar se as APIs de registro não estão bloqueadas na E/S.
- Teste macros de registro com vários padrões, como registro em log de estilo C89, C99.

- Teste as macros de registro em log definindo diferentes níveis de logs, como `Debug`, `Info`, `Error` e `Warning`.

## Transferência de pilha de TCP/IP

Esta seção fornece instruções para fazer a portabilidade e testar pilhas TCP/IP integradas. Se a plataforma descarregar a funcionalidade TCP/IP e TLS em um processador ou módulo de rede separado, você poderá ignorar essa seção de portabilidade e visitar [Fazer portabilidade da Network Transport Interface](#).

O [FreeRTOS+TCP](#) é uma pilha TCP/IP nativa para o kernel do FreeRTOS. O FreeRTOS+TCP é desenvolvido e mantido pela equipe de engenharia do FreeRTOS, e a pilha TCP/IP é recomendada para usar com o FreeRTOS. Para obter mais informações, consulte [Portabilidade do FreeRTOS+TCP](#). Como alternativa, você pode usar a pilha TCP/IP de terceiros [lwIP](#). A instrução de teste fornecida nesta seção usa os testes da interface de transporte para texto simples TCP e não depende da pilha TCP/IP específica implementada.

## Portabilidade do FreeRTOS+TCP

O FreeRTOS+TCP é uma pilha TCP/IP nativa para o kernel do FreeRTOS. Para obter mais informações, consulte [FreeRTOS.org](#).

### Pré-requisitos

Para fazer a portabilidade da biblioteca do FreeRTOS+TCP, é necessário o seguinte:

- Um projeto do IDE que inclui os drivers Ethernet ou Wi-Fi fornecidos pelo fornecedor.

Para obter informações sobre a configuração de um projeto de teste, consulte [Configuração do seu espaço de trabalho e projeto para portabilidade](#).

- Uma configuração validada do kernel do FreeRTOS.

Para obter informações sobre como configurar o kernel do FreeRTOS para sua plataforma, consulte [Configuração de uma porta do kernel do FreeRTOS](#).

### Portabilidade

Antes de começar a fazer a transferência da biblioteca FreeRTOS+TCP, verifique o diretório do [GitHub](#) para ver se já existe uma porta para o dispositivo.

Se não existir uma porta, faça o seguinte:

1. Siga as instruções de [Fazer a portabilidade do FreeRTOS+TCP para um microcontrolador diferente](#) em FreeRTOS.org para fazer a portabilidade do FreeRTOS+TCP para seu dispositivo.
2. Se necessário, siga as instruções de [Fazer a portabilidade do FreeRTOS+TCP para um novo compilador C incorporado](#) em FreeRTOS.org para fazer a portabilidade do FreeRTOS+TCP para um novo compilador.
3. Implemente uma nova porta que use os drivers Ethernet ou Wi-Fi do fornecedor em um arquivo chamado `NetworkInterface.c`. Visite o repositório do [GitHub](#) para obter um modelo.

Depois de criar a porta, ou se já existir uma, crie `FreeRTOSIPConfig.h` e edite as opções de configuração para que estejam corretas para a plataforma. Para obter mais informações sobre as opções de configuração, consulte [Configuração do FreeRTOS+TCP](#) em FreeRTOS.org.

## Testes

Se você usa a biblioteca FreeRTOS+TCP ou uma biblioteca de terceiros, siga as etapas abaixo para testar:

- Forneça uma implementação para APIs `connect/disconnect/send/receive` em testes de interface de transporte.
- Configure um servidor echo no modo de conexão TCP de texto simples e execute testes de interface de transporte.

### Note

Para qualificar oficialmente um dispositivo para FreeRTOS, se sua arquitetura exigir a portabilidade de uma pilha de software TCP/IP, você precisará validar o código-fonte transferido do dispositivo nos testes de interface de transporte no modo de conexão TCP de texto simples no AWS IoT Device Tester. Siga as instruções em [Usar o AWS IoT Device Tester para FreeRTOS](#) no Guia do usuário do FreeRTOS para configurar o AWS IoT Device Tester para validação de porta. Para testar a portabilidade de uma biblioteca específica, o grupo de testes correto deve ser habilitado no arquivo `device.json` na pasta `configs` do Device Tester.

## Portabilidade da biblioteca corePKCS11

O Padrão de criptografia de chave pública #11 define uma API independente de plataforma para gerenciar e usar tokens criptográficos. O [PKCS 11](#) se refere ao padrão e APIs definida por ele. A API criptográfica de PKCS #11 abstrai armazenamento de chaves, propriedades de obtenção/definição para objetos criptográficos e semântica de sessão. É amplamente usado para manipular objetos criptográficos comuns. Suas funções permitem que o software de aplicativo use, crie, modifique e exclua objetos criptográficos, sem expor esses objetos à memória do aplicativo.

As bibliotecas e integrações de referência do FreeRTOS usam um subconjunto do padrão de interface PCKS #11, com foco nas operações que envolvem chaves assimétricas, geração de números aleatórios e hashing. A tabela abaixo lista os casos de uso e as APIs de PKCS #11 necessárias para oferecer suporte.

### Casos de uso

Caso de uso	Família de API com PKCS #11 necessária
Tudo	Initialize, Finalize, Open/Close Session, GetSlotList, Login
Provisionamento	GenerateKeyPair, CreateObject, DestroyObject, initToken, GetTokenInfo
TLS	Random, Sign, FindObject, GetAttributeValue
FreeRTOS+TCP	Random, Digest
OTA	Verificação, resumo, FindObject, GetAttributeValue

### Quando implementar um módulo PKCS #11 completo

O armazenamento de chaves privadas na memória flash de uso geral pode ser conveniente em cenários de avaliação e de prototipagem rápida. Recomendamos o uso de hardware criptográfico dedicado para reduzir as ameaças de roubo de dados e duplicação de dispositivos em cenários de produção. O hardware criptográfico inclui componentes com recursos que impedem que as chaves secretas criptográficas sejam exportadas. Para oferecer suporte a isso, você precisará implementar

um subconjunto de PKCS #11 necessário para trabalhar com bibliotecas FreeRTOS, conforme definido na tabela acima.

## Quando usar a corePKCS11 do FreeRTOS

A biblioteca corePKCS11 contém uma implementação baseada em software da interface PKCS #11 (API) que usa a funcionalidade criptográfica fornecida pelo [TLS Mbed](#). Isso é fornecido para cenários rápidos de prototipagem e avaliação em que o hardware não tem um hardware criptográfico dedicado. Nesse caso, você só precisa implementar a PAL corePKCS11 para fazer com que a implementação baseada em software corePKCS11 funcione com sua plataforma de hardware.

## Portabilidade da corePKCS11

Será necessário ter implementações para ler e gravar objetos criptográficos na memória não volátil (NVM), como a memória flash integrada. Os objetos criptográficos precisam ser armazenados em uma seção da NVM que não tenha sido inicializada e não seja apagada na reprogramação do dispositivo. Os usuários da biblioteca corePKCS11 provisionarão dispositivos com credenciais e reprogramarão o dispositivo com um novo aplicativo que acesse essas credenciais por meio da interface corePKCS11. As portas PAL corePKCS11 devem fornecer um local para armazenar:

- O certificado de cliente do dispositivo
- A chave privada de cliente do dispositivo
- A chave pública de cliente do dispositivo
- Uma CA raiz confiável
- Uma chave pública de verificação de código (ou um certificado que contém a chave pública de verificação de código) para atualizações seguras do carregador de inicializações e sem fios
- Um certificado de provisionamento just-in-time

Inclua [o arquivo de cabeçalho](#) e implemente as APIs PAL definidas.

### APIs PAL

Função	Descrição
PKCS11_PAL_Initialize	Inicializa a camada PAL. Chamado pela biblioteca corePKCS11 no início da sequência de inicialização.



Função	Descrição
PKCS11_PAL_SaveObject	Grava dados no armazenamento não volátil.
PKCS11_PAL_FindObject	Usa um CKA_LABEL PKCS #11 para procurar um objeto PKCS #11 correspondente no armazenamento não volátil e retorna o identificador desse objeto, se existir.
PKCS11_PAL_GetObjectValue	Recupera o valor de um objeto, considerando o identificador.
PKCS11_PAL_GetObjectValueCleanup	Limpeza da chamada PKCS11_PAL_GetObjectValue. Pode ser usada para liberar memória alocada em uma chamada PKCS11_PAL_GetObjectValue.

## Testes

Se você usar a biblioteca corePKCS11 do FreeRTOS ou implementar o subconjunto necessário de APIs de PKCS11, deverá passar nos testes do PKCS11 do FreeRTOS. Eles testam se as funções necessárias para as bibliotecas FreeRTOS funcionam conforme o esperado.

Esta seção também descreve como você pode executar localmente os testes PKCS11 do FreeRTOS com os testes de qualificação.

## Pré-requisitos

Para configurar os testes PKCS11 do FreeRTOS, deve-se implementar o seguinte.

- Uma porta compatível com as APIs PKCS11.
- Uma implementação das funções da plataforma de testes de qualificação do FreeRTOS, que incluem o seguinte:
  - FRTest\_ThreadCreate
  - FRTest\_ThreadTimedJoin
  - FRTest\_MemoryAlloc
  - FRTest\_MemoryFree

(Consulte o arquivo [README.md](#) para os testes de integração de bibliotecas FreeRTOS para PKCS #11 no GitHub.)

## Testes de portabilidade

- Adicione [FreeRTOS-Libraries-Integration-Tests](#) como um submódulo em seu projeto. O submódulo pode ser colocado em qualquer diretório do projeto, desde que possa ser compilado.
- Copie `config_template/test_execution_config_template.h` e `config_template/test_param_config_template.h` para um local do projeto no caminho de compilação e renomeie-os para `test_execution_config.h` e `test_param_config.h`.
- Inclua os arquivos relevantes no sistema de compilação. Se estiver usando CMake, `qualification_test.cmake` e `src/pkcs11_tests.cmake` podem ser usados para incluir os arquivos relevantes.
- Implemente `UNITY_OUTPUT_CHAR` para que os logs de saída do teste e logs do dispositivo não se intercalem.
- Integre o MbedTLS, que verifica o resultado da operação `cryptoki`.
- Chame `RunQualificationTest()` do aplicativo.

## Configuração de testes

O conjunto de testes PKCS11 deve ser configurado de acordo com a implementação do PKCS11. A tabela a seguir lista a configuração exigida pelos testes PKCS11 no arquivo de cabeçalho `test_param_config.h`.

### Configurações de teste PKSC11

Configuração	Descrição
<code>PKCS11_TEST_RSA_KEY_SUPPORT</code>	A portabilidade oferece suporte às funções de chave do RSA.
<code>PKCS11_TEST_EC_KEY_SUPPORT</code>	A portabilidade oferece suporte às funções de chave de EC.
<code>PKCS11_TEST_IMPORT_PRIVATE_KEY_SUPPORT</code>	A portabilidade oferece suporte à importação da chave privada. A importação de chaves

Configuração	Descrição
	RSA e EC é validada no teste se o suporte às funções de chave estiver habilitado.
PKCS11_TEST_GENERATE_KEYPAIR_SUPPORT	A portabilidade oferece suporte à geração de pares de chaves. A geração de pares de chaves EC é validada no teste se o suporte às funções de chave estiver habilitado.
PKCS11_TEST_PREPROVISIONED_SUPPORT	A portabilidade tem credenciais pré-provisionadas. PKCS11_TEST_LABEL_DEVICE_PRIVATE_KEY_FOR_TLS , PKCS11_TEST_LABEL_DEVICE_PUBLIC_KEY_FOR_TLS e PKCS11_TEST_LABEL_DEVICE_CERTIFICATE_FOR_TLS , são exemplos das credenciais.
PKCS11_TEST_LABEL_DEVICE_PRIVATE_KEY_FOR_TLS	O rótulo da chave privada usada no teste.
PKCS11_TEST_LABEL_DEVICE_PUBLIC_KEY_FOR_TLS	O rótulo da chave pública usada no teste.
PKCS11_TEST_LABEL_DEVICE_CERTIFICATE_FOR_TLS	O rótulo do certificado usado no teste.
PKCS11_TEST_JITP_CODEVERIFY_ROOT_CERT_SUPPORTED	A portabilidade oferece suporte ao armazenamento de JITP. Defina isso como 1 para ativar o teste <code>codeverify</code> de JITP.
PKCS11_TEST_LABEL_CODE_VERIFICATION_KEY	O rótulo da chave de verificação de código usada no teste <code>codeverify</code> de JITP.
PKCS11_TEST_LABEL_JITP_CERTIFICATE	O rótulo do certificado JITP usado no teste <code>codeverify</code> de JITP.
PKCS11_TEST_LABEL_ROOT_CERTIFICATE	O rótulo do certificado raiz usado no teste <code>codeverify</code> de JITP.


As bibliotecas e integrações de referência do FreeRTOS devem oferecer suporte a no mínimo uma configuração de função de chave, como chaves de Curva elíptica ou RSA, e um mecanismo de provisionamento de teclas compatível com as APIs de PKCS11. O teste deve habilitar as seguintes configurações:

- Pelo menos uma das configurações de função de chave a seguir:
  - PKCS11\_TEST\_RSA\_KEY\_SUPPORT
  - PKCS11\_TEST\_EC\_KEY\_SUPPORT
- Pelo menos uma das configurações de provisionamento de chave a seguir:
  - PKCS11\_TEST\_IMPORT\_PRIVATE\_KEY\_SUPPORT
  - PKCS11\_TEST\_GENERATE\_KEYPAIR\_SUPPORT
  - PKCS11\_TEST\_PREPROVISIONED\_SUPPORT

O teste de credencial do dispositivo pré-provisionado deve ser executado sob as seguintes condições:

- PKCS11\_TEST\_PREPROVISIONED\_SUPPORT devem estar habilitados e outros mecanismos de provisionamento desativados.
- Ter somente uma função de chave, PKCS11\_TEST\_RSA\_KEY\_SUPPORT ou PKCS11\_TEST\_EC\_KEY\_SUPPORT está ativada.
- Configure os rótulos de chave pré-provisionados de acordo com a função de chave, incluindo PKCS11\_TEST\_LABEL\_DEVICE\_PRIVATE\_KEY\_FOR\_TLS, PKCS11\_TEST\_LABEL\_DEVICE\_PUBLIC\_KEY\_FOR\_TLS e PKCS11\_TEST\_LABEL\_DEVICE\_CERTIFICATE\_FOR\_TLS. Essas credenciais devem existir antes de executar o teste.

É aconselhável executar o teste várias vezes em configurações diferentes, se a implementação oferecer suporte a credenciais pré-provisionadas e outros mecanismos de provisionamento.

 Note

Os objetos com rótulos PKCS11\_TEST\_LABEL\_DEVICE\_PRIVATE\_KEY\_FOR\_TLS, PKCS11\_TEST\_LABEL\_DEVICE\_PUBLIC\_KEY\_FOR\_TLS e PKCS11\_TEST\_LABEL\_DEVICE\_CERTIFICATE\_FOR\_TLS serão destruídos

durante o teste se `PKCS11_TEST_GENERATE_KEYPAIR_SUPPORT` ou `PKCS11_TEST_GENERATE_KEYPAIR_SUPPORT` estiverem habilitados.

## Execução de testes

Esta seção descreve como você pode testar localmente a interface de PKCS11 com os testes de qualificação. Como alternativa, você também pode usar o IDT para automatizar a execução. Consulte o [AWS IoT Device Tester para o FreeRTOS](#) no Guia do usuário do FreeRTOS para obter detalhes.

As instruções a seguir descrevem como executar os testes:

- Abra `test_execution_config.h` e defina `CORE_PKCS11_TEST_ENABLED` como 1.
- Compile e atualize o aplicativo em seu dispositivo para ser executado. Os resultados do teste são enviados para a porta serial.

Confira a seguir um exemplo do resultado do teste de saída.

```
TEST(Full_PKCS11_StartFinish, PKCS11_StartFinish_FirstTest) PASS
TEST(Full_PKCS11_StartFinish, PKCS11_GetFunctionList) PASS
TEST(Full_PKCS11_StartFinish, PKCS11_InitializeFinalize) PASS
TEST(Full_PKCS11_StartFinish, PKCS11_GetSlotList) PASS
TEST(Full_PKCS11_StartFinish, PKCS11_OpenSessionCloseSession) PASS
TEST(Full_PKCS11_Capabilities, PKCS11_Capabilities) PASS
TEST(Full_PKCS11_NoObject, PKCS11_Digest) PASS
TEST(Full_PKCS11_NoObject, PKCS11_Digest_ErrorConditions) PASS
TEST(Full_PKCS11_NoObject, PKCS11_GenerateRandom) PASS
TEST(Full_PKCS11_NoObject, PKCS11_GenerateRandomMultiThread) PASS
TEST(Full_PKCS11_RSA, PKCS11_RSA_CreateObject) PASS
TEST(Full_PKCS11_RSA, PKCS11_RSA_FindObject) PASS
TEST(Full_PKCS11_RSA, PKCS11_RSA_GetAttributeValue) PASS
TEST(Full_PKCS11_RSA, PKCS11_RSA_Sign) PASS
TEST(Full_PKCS11_RSA, PKCS11_RSA_FindObjectMultiThread) PASS
TEST(Full_PKCS11_RSA, PKCS11_RSA_GetAttributeValueMultiThread) PASS
TEST(Full_PKCS11_RSA, PKCS11_RSA_DestroyObject) PASS
TEST(Full_PKCS11_EC, PKCS11_EC_GenerateKeyPair) PASS
TEST(Full_PKCS11_EC, PKCS11_EC_CreateObject) PASS
TEST(Full_PKCS11_EC, PKCS11_EC_FindObject) PASS
TEST(Full_PKCS11_EC, PKCS11_EC_GetAttributeValue) PASS
```

```
TEST(Full_PKCS11_EC, PKCS11_EC_Sign) PASS
TEST(Full_PKCS11_EC, PKCS11_EC_Verify) PASS
TEST(Full_PKCS11_EC, PKCS11_EC_FindObjectMultiThread) PASS
TEST(Full_PKCS11_EC, PKCS11_EC_GetAttributeValueMultiThread) PASS
TEST(Full_PKCS11_EC, PKCS11_EC_SignVerifyMultiThread) PASS
TEST(Full_PKCS11_EC, PKCS11_EC_DestroyObject) PASS
```

```
-----
27 Tests 0 Failures 0 Ignored
OK
```

O teste será concluído quando todos os testes forem aprovados.

### Note

Para qualificar oficialmente um dispositivo para o FreeRTOS, é necessário validar o código-fonte transferido do dispositivo com o AWS IoT Device Tester. Siga as instruções em [Usar o AWS IoT Device Tester para FreeRTOS](#) no Guia do usuário do FreeRTOS para configurar o AWS IoT Device Tester para validação de porta. Para testar a portabilidade de uma biblioteca específica, o grupo de testes correto deve ser habilitado no arquivo `device.json` na pasta do AWS IoT Device Tester `configs`.

## Fazer portabilidade da Network Transport Interface

### Integração da biblioteca TLS

Para autenticação Transport Layer Security (TLS), use a pilha TLS de sua preferência. Recomendamos usar o [Mbed TLS](#) porque ele é testado com bibliotecas FreeRTOS. Você pode descobrir um exemplo disso neste repositório do [GitHub](#).

Independentemente da implementação de TLS usada pelo seu dispositivo, você deve implementar os hooks de transporte subjacentes para a pilha TLS com a pilha TCP/IP. Eles devem oferecer suporte aos [pacotes de criptografia TLS que são compatíveis com o AWS IoT](#).

### Fazer portabilidade da biblioteca Network Transport Interface

Você deve implementar uma interface de transporte de rede para usar [coreMQTT](#) e [coreHTTP](#). A interface de transporte de rede contém ponteiros de função e dados de contexto necessários para

enviar e receber dados em uma única conexão de rede. Consulte [Interface de transporte](#) para obter mais detalhes. O FreeRTOS fornece um conjunto de testes integrados de interface de transporte de rede para validar essas implementações. A seção a seguir orienta você sobre como configurar seu projeto para executar esses testes.

## Pré-requisitos

Para fazer a portabilidade desse teste, é necessário:

- Um projeto com um sistema de compilação que pode criar o FreeRTOS com uma porta validada do kernel do FreeRTOS.
- Implementação funcional de drivers de rede.

## Portabilidade

- Adicione [Freertos-Libraries-Integration-Tests](#) como um submódulo em seu projeto. Não importa onde o submódulo será colocado no projeto, desde que ele possa ser compilado.
- Copie `config_template/test_execution_config_template.h` e `config_template/test_param_config_template.h` para um local do projeto no caminho de compilação e renomeie-os para `test_execution_config.h` e `test_param_config.h`.
- Inclua os arquivos relevantes no sistema de compilação. Se estiver usando CMake, `qualification_test.cmake` e `src/transport_interface_tests.cmake` são usados para incluir os arquivos relevantes.
- Implemente as seguintes funções em um local apropriado do projeto:
  - `Rnetwork connect function`: a assinatura é definida por `NetworkConnectFunc` em `src/common/network_connection.h`. Essa função usa um ponteiro para o contexto da rede, um ponteiro para as informações do host e um ponteiro para as credenciais da rede. Ela estabelece uma conexão com o servidor especificado nas informações do host com as credenciais de rede fornecidas.
  - `Rnetwork disconnect function`: a assinatura é definida por `NetworkDisconnectFunc` em `src/common/network_connection.h`. Essa função usa um ponteiro para um contexto de rede. Ela desconecta uma conexão previamente estabelecida armazenada no contexto da rede.
  - `setupTransportInterfaceTestParam()`: esta API é definida em `src/transport_interface/transport_interface_tests.h`. A implementação deve ter

exatamente o mesmo nome e assinatura definidos em `transport_interface_tests.h`. Essa função recebe um ponteiro para uma estrutura `TransportInterfaceTestParam`. Ela preencherá os campos na estrutura `TransportInterfaceTestParam` que é usada pelo teste da interface de transporte.

- Implemente `UNITY_OUTPUT_CHAR` para que os logs de saída do teste não intercalem com os logs do dispositivo.
- Chame `runQualificationTest()` do aplicativo. O hardware do dispositivo deve ser inicializado corretamente e a rede deve estar conectada antes da chamada.

## Gerenciamento de credenciais (chave gerada no dispositivo)

Quando `FORCE_GENERATE_NEW_KEY_PAIR` em `test_param_config.h` é definido como 1, o aplicativo do dispositivo gera um novo par de chaves no dispositivo e gera a chave pública. O aplicativo do dispositivo usa `ECHO_SERVER_ROOT_CA` e `TRANSPORT_CLIENT_CERTIFICATE` como certificado da CA raiz do servidor echo e do cliente ao estabelecer uma conexão TLS com o servidor echo. O IDT define esses parâmetros durante a execução da qualificação.

## Gerenciamento de credenciais (chave de importação)

O aplicativo do dispositivo usa `ECHO_SERVER_ROOT_CA`, `TRANSPORT_CLIENT_CERTIFICATE` e `TRANSPORT_CLIENT_PRIVATE_KEY` em `test_param_config.h` como certificado da CA raiz do servidor echo, certificado de cliente e chave privada de cliente ao estabelecer uma conexão TLS com o servidor echo. O IDT define esses parâmetros durante a execução da qualificação.

## Testes

Esta seção descreve como você pode testar localmente a interface de transporte com os testes de qualificação. Detalhes adicionais podem ser encontrados no arquivo `README.md` fornecido na seção [transport\\_interface](#) do `FreeRTOS-Libraries-Integration-Tests` no GitHub.

Como alternativa, você também pode usar o IDT para automatizar a execução. Consulte o [AWS IoT Device Tester para o FreeRTOS](#) no Guia do usuário do FreeRTOS para obter detalhes.

## Habilitação do teste

Abra `test_execution_config.h` e defina `TRANSPORT_INTERFACE_TEST_ENABLED` como 1.



## Configuração do servidor echo para testes

É necessário ter um servidor echo acessível a partir do dispositivo que executa os testes para fazer testes locais. O servidor echo deve oferecer suporte ao TLS se a implementação da interface de transporte oferecer suporte ao TLS. Se você ainda não tem um, o repositório GitHub [Freertos-libraries-integration-tests](#) tem uma implementação de servidor echo.

## Configuração do projeto para teste

Em `test_param_config.h`, atualize `ECHO_SERVER_ENDPOINT` e `ECHO_SERVER_PORT` para a configuração do endpoint e do servidor na etapa anterior.

## Credenciais de configuração (chave gerada no dispositivo)

- Defina `ECHO_SERVER_ROOT_CA` como o certificado do servidor echo.
- Defina `FORCE_GENERATE_NEW_KEY_PAIR` como 1 para gerar um par de chaves e obter a chave pública.
- Defina `FORCE_GENERATE_NEW_KEY_PAIR` como 0 novamente após a geração da chave.
- Use a chave pública e do servidor e o certificado para gerar o certificado do cliente.
- Defina `TRANSPORT_CLIENT_CERTIFICATE` como o certificado de cliente gerado.

## Credenciais de configuração (chave de importação)

- Defina `ECHO_SERVER_ROOT_CA` como o certificado do servidor echo.
- Defina `TRANSPORT_CLIENT_CERTIFICATE` como o certificado de cliente pré-gerado.
- Defina `TRANSPORT_CLIENT_PRIVATE_KEY` como a chave privada pré-gerada do cliente.

## Compilação e instalação do aplicativo

Compile e instale o aplicativo usando a cadeia de ferramentas de sua escolha. Quando `runQualificationTest()` for invocado, os testes da interface de transporte serão executados. Os resultados do teste são emitidos para a porta serial.

### Note

Para qualificar oficialmente um dispositivo para o FreeRTOS, você deve validar o código-fonte transferido do dispositivo nos grupos de teste OTA PAL e OTA E2E com o AWS IoT

Device Tester. Siga as instruções em [Usar o AWS IoT Device Tester Device Tester para o FreeRTOS](#) no Guia do usuário do FreeRTOS para configurar o AWS IoT Device Tester para validação de portabilidade. Para testar a portabilidade de uma biblioteca específica, o grupo de testes correto deve ser habilitado no arquivo `device.json` na pasta do AWS IoT Device Tester configs.

## Configuração da biblioteca coreMQTT

Os dispositivos na borda podem usar o protocolo MQTT para se comunicar com a Nuvem AWS. O AWS IoT hospeda um agente MQTT que recebe e envia mensagens para dispositivos conectados na borda.

A biblioteca coreMQTT implementa o protocolo MQTT para dispositivos que executam o . A biblioteca coreMQTT não precisa ser transferida, mas o projeto de teste do dispositivo deve passar em todos os testes MQTT para qualificação. Para obter mais informações, consulte [Biblioteca coreMQTT](#) no Guia do usuário do FreeRTOS.

### Pré-requisitos

Para configurar os testes da biblioteca coreMQTT, você precisa de uma porta de interface de transporte de rede. Para saber mais, consulte [Fazer portabilidade da Network Transport Interface](#).

### Testes

Execute testes de integração da coreMQTT:

- Registre seu certificado de cliente no agente MQTT.
- Configure o endpoint do agente em `config` e execute os testes de integração.

### Criação de demonstração de referência do MQTT

Recomendamos usar o agente coreMQTT para lidar com a segurança de thread em todas as operações do MQTT. O usuário também precisará publicar e assinar tarefas e testes do Device Advisor para validar se o aplicativo integra TLS, MQTT e outras bibliotecas FreeRTOS de forma eficaz.

Para qualificar oficialmente um dispositivo para FreeRTOS, valide seu projeto de integração com os casos de teste da MQTT do AWS IoT Device Tester. Consulte o [fluxo de trabalho do AWS IoT](#)

[Device Advisor](#) para obter instruções de configuração e teste. Os casos de teste obrigatórios para TLS e MQTT estão listados abaixo:

#### Casos de teste do TLS

Caso de teste	Casos de teste	Testes necessários
TLS	Conexão TLS	Sim
TLS	Pacotes de criptografia de suporte ao TLS do AWS IoT	Um <a href="#">pacote de criptografia</a> recomendado
TLS	Certificado de servidor TLS desprotegido	Sim
TLS	TLS: certificado do servidor de nome de assunto incorreto	Sim

#### Casos de teste do MQTT

Caso de teste	Casos de teste	Testes necessários
MQTT	MQTT Connect	Sim
MQTT	Novas tentativas de tremulação de conexão MQTT	Sim, sem avisos
MQTT	MQTT Subscribe	Sim
MQTT	MQTT Publish	Sim
MQTT	QoS 1 ClientPuback de MQTT	Sim
MQTT	No Ack PingResp de MQTT	Sim

## Configuração da biblioteca coreHTTP

Os dispositivos na borda podem usar o protocolo HTTP para se comunicar com a nuvem da AWS. Os serviços do AWS IoT hospedam um servidor HTTP que envia e recebe mensagens para dispositivos conectados na borda.

### Testes

Siga as etapas abaixo para testar:

- Configure a PKI para autenticação mútua TLS na AWS ou um servidor HTTP.
- Execute testes de integração da coreHTTP.

## Portabilidade da biblioteca de atualização sem fios do AWS IoT

É possível fazer o seguinte com atualizações sem fios do FreeRTOS:

- Implante novas imagens de firmware em um único dispositivo, um grupo de dispositivos ou toda a sua frota.
- Implantar firmware em dispositivos conforme eles são adicionados a grupos, redefinidos ou provisionados novamente.
- Verifique a autenticidade e a integridade do novo firmware depois da sua implantação nos dispositivos.
- Monitore o progresso de uma implantação.
- Depure uma implantação com falha.
- Assine digitalmente o firmware usando o Code Signing para AWS IoT.

Para obter mais informações, consulte as [Atualizações sem fios do FreeRTOS](#) no Guia do usuário do FreeRTOS junto com a [Documentação de atualização sem fios do AWS IoT](#).

Você pode usar a biblioteca de atualização OTA para integrar a funcionalidade OTA nos aplicativos do FreeRTOS. Para obter mais informações, consulte [Biblioteca de atualização OTA do FreeRTOS](#) no Guia do usuário do FreeRTOS.

Os dispositivos do FreeRTOS devem impor a verificação criptográfica de assinatura de código nas imagens de firmware OTA que recebem. Recomendamos os seguintes algoritmos:

- Algoritmo de assinatura digital de curva elíptica (ECDSA)
- Curva NIST P256
- Hash SHA-256

## Pré-requisitos

- Complete as instruções em [Configuração do seu espaço de trabalho e projeto para portabilidade](#).
- Crie uma porta de interface de transporte de rede.

Para obter mais informações, consulte [Fazer portabilidade da Network Transport Interface](#).

- Integre a biblioteca coreMQTT. Consulte [Biblioteca coreMQTT](#) no Guia do usuário do FreeRTOS.
- Crie um carregador de inicialização que ofereça suporte a atualizações OTA.

## Portabilidade de plataforma

Você deve fornecer uma implementação da camada de abstração portátil (PAL) OTA para transferir a biblioteca OTA para um novo dispositivo. As APIs PAL são definidas no arquivo [ota\\_platform\\_interface.h](#) para o qual devem ser fornecidos detalhes específicos da implementação.

Nome da função	Descrição
<code>otaPal_Abort</code>	Interrompe uma atualização OTA.
<code>otaPal_CreateFileForRx</code>	Cria um arquivo para armazenar os blocos de dados recebidos.
<code>otaPal_CloseFile</code>	Fecha o arquivo especificado. Isso pode autenticar o arquivo se você usar armazenamento que implementa a proteção criptográfica.
<code>otaPal_WriteBlock</code>	Grava um bloco de dados no arquivo especificado no deslocamento determinado. A função retornará o número de bytes gravados quando tiver êxito. Caso contrário, a função retornará um código de erro negativo. O tamanho do bloco sempre será uma potência de dois e

Nome da função	Descrição
	será alinhado. Para obter mais informações, consulte <a href="#">Configuração da biblioteca OTA</a> .
<code>otaPal_ActivateNewImage</code>	Ativa ou inicia a nova imagem de firmware. Em algumas portas, se o dispositivo for redefinido o programaticamente de forma síncrona, essa função poderá não retornar.
<code>otaPal_SetPlatformImageState</code>	Faz o que é exigido pela plataforma para aceitar ou rejeitar a imagem de firmware (ou pacote) OTA mais recente. Para implementar essa função, consulte a documentação para obter os detalhes e a arquitetura da sua placa (plataforma).
<code>otaPal_GetPlatformImageState</code>	Obtém o estado da imagem de atualização OTA.

Implemente as funções nesta tabela se o dispositivo tiver suporte integrado para elas.

Nome da função	Descrição
<code>otaPal_CheckFileSignature</code>	Verifica a assinatura do arquivo especificado.
<code>otaPal_ReadAndAssumeCertificate</code>	Lê o certificado do assinante especificado no sistema de arquivos e o retorna para o chamador.
<code>otaPal_ResetDevice</code>	Redefine o dispositivo.

**Note**

Certifique-se de que você tem um bootloader que pode oferecer suporte a atualizações OTA. Para obter instruções sobre como criar o carregador de inicialização do dispositivo do AWS IoT, consulte [Bootloader de dispositivo de IoT](#).

## Testes E2E e PAL

Execute testes PAL OTA e E2E.

### Testes E2E

O teste de ponta a ponta (E2E) OTA é usado para verificar a capacidade OTA de um dispositivo e simular cenários reais. Esse teste incluirá tratamento de erros.

#### Pré-requisitos

Para fazer a portabilidade desse teste, é necessário:

- Um projeto com uma biblioteca OTA da AWS integrada. Visite o [Guia de portabilidade da biblioteca OTA](#) para obter informações adicionais.
- Faça a portabilidade do aplicativo de demonstração usando a biblioteca OTA para interagir com o AWS IoT Core e fazer as atualizações OTA. Consulte [Portabilidade do aplicativo de demonstração OTA](#).
- Configure a ferramenta do IDT. Isso executa o aplicativo host E2E OTA para compilar, instalar e monitorar o dispositivo em diferentes configurações e valida a integração da biblioteca OTA.

#### Portabilidade do aplicativo de demonstração OTA

O teste E2E OTA deve ter um aplicativo de demonstração OTA para validar a integração da biblioteca OTA. O aplicativo de demonstração deve ter a capacidade de realizar atualizações de firmware OTA. Você pode encontrar o aplicativo de demonstração OTA do FreeRTOS no repositório [GitHub do FreeRTOS](#). Recomendamos que você use o aplicativo de demonstração como referência e o modifique de acordo com suas especificações.

#### Etapas da portabilidade

1. Inicialize o agente OTA.

2. Implemente a função de retorno de chamada do aplicativo OTA.
3. Crie a tarefa de processamento de eventos do agente OTA.
4. Inicie o agente OTA.
5. Monitore as estatísticas do agente OTA.
6. Encerre o agente OTA.

Visite [OTA do FreeRTOS por MQTT - Ponto de entrada da demonstração](#) para obter instruções detalhadas.

## Configuração

As seguintes configurações são necessárias para interagir com o AWS IoT Core:

- Credenciais de cliente do AWS IoT Core
  - Configure DemoConfigRoot\_CA\_PEM em `Ota_Over_Mqtt_Demo/demo_config.h` com os Endpoint dos serviços de confiança da Amazon. Consulte [Autenticação do servidor da AWS](#) para obter mais detalhes.
  - Configure `democonfigCLIENT_CERTIFICATE_PEM` e `democonfigCLIENT_PRIVATE_KEY_PEM` em `Ota_Over_Mqtt_Demo/demo_config.h` com suas credenciais de cliente AWS IoT. Consulte os [detalhes da autenticação do cliente da AWS](#) para saber mais sobre certificados e chaves privadas do cliente.
- Versão do aplicativo
- Protocolo de controle OTA
- Protocolo de dados OTA
- Credenciais de assinatura de código
- Outras configurações da biblioteca OTA

Você pode encontrar as informações anteriores nos aplicativos de demonstração OTA do FreeRTOS em `demo_config.h` e `ota_config.h`. Visite [OTA do FreeRTOS por MQTT - Configuração do dispositivo](#) para obter mais informações.

## Verificação de compilação

Execute o aplicativo de demonstração para executar o trabalho OTA. Quando isso for concluído com êxito, você poderá continuar executando os testes E2E OTA.



A [demonstração OTA](#) do FreeRTOS fornece informações detalhadas sobre como configurar um cliente OTA e um trabalho OTA do AWS IoT Core no simulador do Windows da AWS do FreeRTOS. OTA é compatível com os protocolos MQTT e HTTP. Consulte os exemplos a seguir para obter mais detalhes:

- [Demonstração OTA por MQTT no simulador do Windows](#)
- [Demonstração OTA por HTTP no simulador do Windows](#)

### Execução de testes com a ferramenta do IDT

Para executar os testes E2E OTA, você deve usar o AWS IoT Device Tester (IDT) para automatizar a execução. Consulte o [AWS IoT Device Tester para o FreeRTOS](#) no Guia do usuário do FreeRTOS para obter mais detalhes.

### Casos de teste E2E

Caso de teste	Descrição
OTAE2EGreaterVersion	Teste "caminho feliz" para atualizações regulares do OTA. Ele cria uma atualização com uma versão mais recente, que o dispositivo atualiza com êxito.
OTAE2EBackToBackDownloads	Esse teste cria três atualizações OTA consecutivas. O esperado é que o dispositivo atualize três vezes consecutivas.
OTAE2ERollbackIfUnableToConnectAfterUpdate	Esse teste verifica se o dispositivo é revertido para o firmware anterior se não conseguir se conectar à rede com o novo firmware.
OTAE2ESameVersion	Esse teste confirma que o dispositivo rejeita o firmware de entrada se a versão permanecer a mesma.
OTAE2EUnsignedImage	Esse teste verifica se o dispositivo rejeita uma atualização se a imagem não estiver assinada.

Caso de teste	Descrição
OTAE2EUntrustedCertificate	Esse teste verifica se o dispositivo rejeita uma atualização se o firmware estiver assinado com um certificado não confiável.
OTAE2EPreviousVersion	Esse teste verifica se o dispositivo rejeita uma versão de atualização mais antiga.
OTAE2EIncorrectSigningAlgorithm	Dispositivos diferentes oferecem suporte a algoritmos de assinatura e hashing diferentes. Esse teste verifica se o dispositivo falha na atualização OTA, caso ele seja criado com um algoritmo não compatível.
OTAE2EDisconnectResume	Este é o teste de "caminho feliz" para o atributo de suspensão e retomada. Esse teste cria uma atualização OTA e inicia a atualização. Em seguida, ele se conecta ao AWS IoT Core com o mesmo ID de cliente (nome de coisa) e credenciais. do AWS IoT Core, em seguida, desconecta o dispositivo. O esperado é que o dispositivo detecte que está desconectado do AWS IoT Core e, após um período, passe para um estado suspenso e tente se reconectar ao AWS IoT Core e retomar o download.

Caso de teste	Descrição
OTA2E2DisconnectCancelUpdate	<p>Esse teste verifica se o dispositivo pode se recuperar, caso o trabalho OTA seja cancelado enquanto está em um estado suspenso. Ele faz a mesma coisa que o teste OTA2E2DisconnectResume, exceto que depois de se conectar ao dispositivo do AWS IoT Core, que desconecta o dispositivo, ele cancela a atualização OTA. Uma nova atualização é criada. O esperado é que o dispositivo se reconecte ao AWS IoT Core, anule a atualização atual, volte ao estado de espera e aceite e conclua a próxima atualização.</p>
OTA2E2PresignedUrlExpired	<p>Quando uma atualização OTA é criada, você pode configurar a vida útil do URL pré-assinado do S3. Esse teste verifica se o dispositivo é capaz de realizar um OTA, mesmo que não consiga concluir o download quando o URL expirar. O esperado é que o dispositivo solicite um novo documento de trabalho, que contém um novo URL para retomar o download.</p>
OTA2E2UpdatesCancel1st	<p>Esse teste cria duas atualizações OTA consecutivas. Quando o dispositivo relata que está baixando a primeira atualização, o teste força o cancelamento da primeira atualização. O esperado é que o dispositivo anule a atualização atual, detecte a segunda atualização e a conclua.</p>

Caso de teste	Descrição
OTA_E2E_CancelThenUpdate	Esse teste cria duas atualizações OTA consecutivas. Quando o dispositivo relata que está baixando a primeira atualização, o teste força o cancelamento da primeira atualização. O esperado é que o dispositivo anule a atualização atual e detecte a segunda atualização, depois a conclua.
OTA_E2E_ImageCrashed	Esse teste verifica se o dispositivo é capaz de rejeitar uma atualização quando a imagem falha.

## Testes PAL

### Pré-requisitos

Para transferir os testes da interface de transporte de rede, será necessário:

- Um projeto que pode compilar o FreeRTOS com uma porta kernel válida do FreeRTOS.
- Uma implementação funcional do PAL OTA.

### Portabilidade

- Adicione [Freertos-Libraries-Integration-Tests](#) como um submódulo em seu projeto. O submódulo deve ser localizado no projeto onde ele possa ser compilado.
- Copie `config_template/test_execution_config_template.h` e `config_template/test_param_config_template.h` para um local no caminho de compilação e renomeie-os para `test_execution_config.h` e `test_param_config.h`.
- Inclua os arquivos relevantes no sistema de compilação. Se estiver usando CMake, `qualification_test.cmake` e `src/ota_pal_tests.cmake` podem ser usados para incluir os arquivos relevantes.
- Configure o teste implementando as seguintes funções:

- `SetupOtaPalTestParam()` definido em `src/ota/ota_pal_test.h`. A implementação deve ter exatamente o mesmo nome e assinatura definidos em `ota_pal_test.h`. No momento, não é necessário configurar essa função.
- Implemente `UNITY_OUTPUT_CHAR` para que os logs de saída do teste não intercalem com os logs do dispositivo.
- Chame `RunQualificationTest()` do aplicativo. O hardware do dispositivo deve ser inicializado corretamente e a rede deve estar conectada antes da chamada.

## Testes

Esta seção descreve os testes locais dos testes de qualificação PAL OTA.

### Habilitação do teste

Abra `test_execution_config.h` e defina `OTA_PAL_TEST_ENABLED` como 1.

Em `test_param_config.h`, atualize as seguintes opções:

- `OTA_PAL_TEST_CERT_TYPE`: selecione o tipo de certificado usado.
- `OTA_PAL_CERTIFICATE_FILE`: caminho para o certificado do dispositivo, se aplicável.
- `OTA_PAL_FIRMWARE_FILE`: nome do arquivo de firmware, se aplicável.
- `OTA_PAL_USE_FILE_SYSTEM`: defina como 1 se o PAL OTA usar abstração do sistema de arquivos.

Compile e instale o aplicativo usando uma cadeia de ferramentas de sua escolha. Quando `RunQualificationTest()` for chamado, os testes PAL OTA serão executados. Os resultados do teste são enviados para a porta serial.

## Integração de tarefas OTA

- Adicione o agente OTA à demonstração atual do MQTT.
- Execute testes de ponta a ponta (E2E) OTA com o AWS IoT. Isso verifica se a integração está funcionando conforme esperado.

**Note**

Para qualificar oficialmente um dispositivo para FreeRTOS, você deve validar o código-fonte transferido do dispositivo nos grupos de teste PAL OTA e E2E OTA com o AWS IoT Device Tester. Siga as instruções em [Usar o AWS IoT Device Tester Device Tester para o FreeRTOS](#) no Guia do usuário do FreeRTOS para configurar o AWS IoT Device Tester para validação de porta. Para testar a portabilidade de uma biblioteca específica, o grupo de testes correto deve ser habilitado no arquivo `device.json` na pasta do AWS IoT Device Tester configs.

## Bootloader de dispositivo de IoT

Você deve fornecer o próprio aplicativo de carregamento de inicialização seguro. Verifique se o design e a implementação fornecem uma mitigação adequada das ameaças à segurança. A seguir confira a modelagem de ameaças para sua referência.

### Modelagem de ameaças para o bootloader de dispositivos de IoT

#### Contexto

Como uma definição de trabalho, os dispositivos do AWS IoT incorporados referenciados por esse modelo de ameaça são produtos baseados em microcontroladores que interagem com serviços em nuvem. Eles podem ser implantados em ambientes de consumo, comerciais ou industriais. Os dispositivos de IoT podem coletar dados sobre um usuário, um paciente, uma máquina ou um ambiente, além de poderem controlar qualquer coisa, desde lâmpadas e fechaduras de porta até máquinas de fábrica.

A modelagem de ameaças é uma abordagem da segurança do ponto de vista de um adversário hipotético. Considerando as metas e os métodos do adversário, uma lista de ameaças é criada. Ameaças são ataques contra um recurso ou ativo executado por um adversário. A lista é priorizada e usada para identificar ou criar soluções de mitigações. Ao escolher uma solução de mitigação, o custo de implementá-la e mantê-la deve ser equilibrado com o valor real de segurança que ela fornece. Existem várias [metodologias de modelos de ameaças](#). Todas elas são capazes de ajudar o desenvolvimento de um produto de AWS IoT seguro e bem-sucedido.

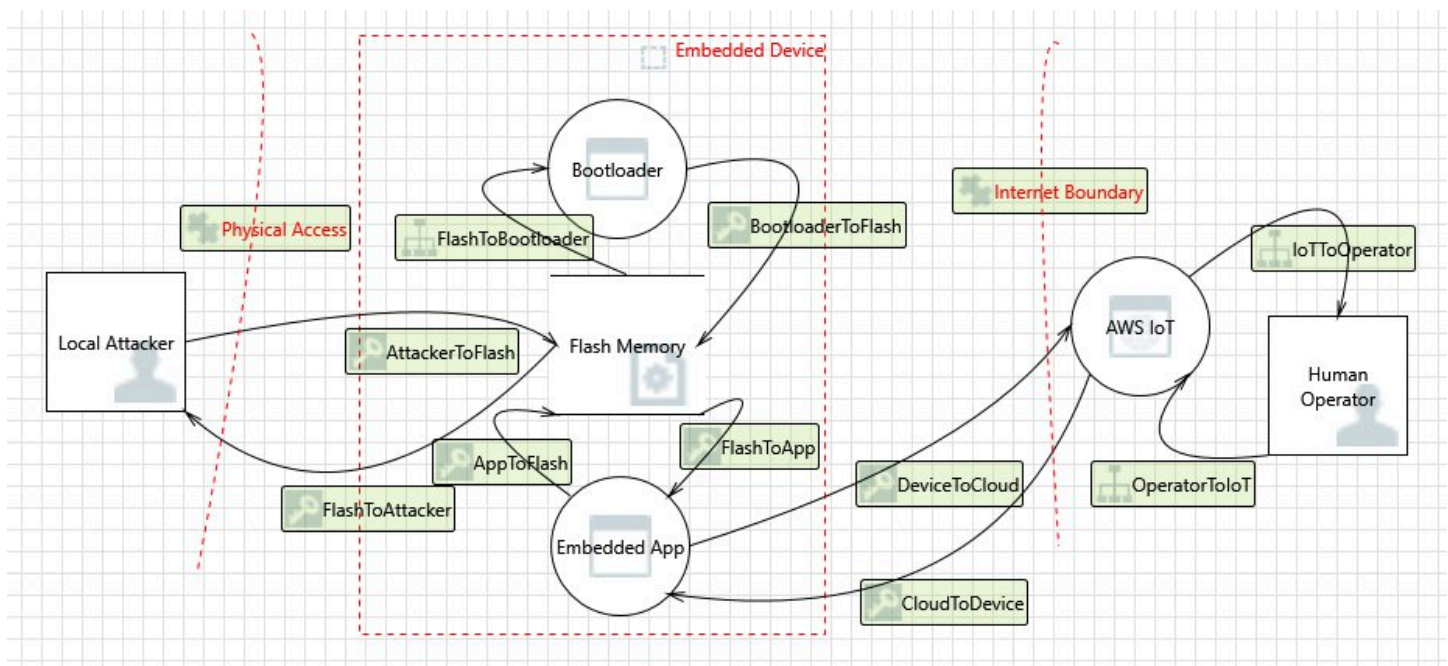
O FreeRTOS oferece atualizações de software OTA (sem fios) para dispositivos AWS IoT. O recurso de atualização combina serviços em nuvem com bibliotecas de software no dispositivo e

um bootloader fornecido pelo parceiro. Esse modelo de ameaça se concentra especificamente em ameaças contra o bootloader.

### Casos de uso do bootloader

- Assine e criptografe digitalmente o firmware antes da implantação.
- Implante novas imagens de firmware em um único dispositivo, um grupo de dispositivos ou toda a frota.
- Verifique a autenticidade e a integridade do novo firmware depois de implantá-lo nos dispositivos.
- Os dispositivos só executam software não modificado de uma origem confiável.
- Os dispositivos são resilientes a software com falha recebido por meio do OTA.

### Diagrama de fluxo de dados



### Ameaças

Alguns ataques têm vários modelos de mitigação; por exemplo, um man-in-the-middle da rede destinado a entregar uma imagem de firmware mal-intencionada é atenuado pela verificação da confiança no certificado oferecido pelo servidor TLS e no certificado de verificação de assinatura da nova imagem de firmware. Para maximizar a segurança do carregador de inicialização, toda solução de mitigação que não sejam dele será considerada não confiável. O carregador de inicialização deve ter soluções de mitigação intrínsecas para cada ataque. Ter soluções de mitigação em camadas é conhecido como defesa completa.

## Ameaças:

- Um invasor sequestra a conexão do dispositivo com o servidor para entregar uma imagem de firmware mal-intencionada.

### Exemplo de atenuação

- Na inicialização, o bootloader verifica a assinatura criptográfica da imagem usando um certificado conhecido. Se a verificação falhar, o bootloader reverterá para a imagem anterior.
- Um invasor explora um estouro de buffer para introduzir comportamento mal-intencionado na imagem de firmware existente armazenada em flash.

### Exemplos de atenuação

- Na inicialização, o bootloader verifica, conforme descrito anteriormente. Quando a verificação falha sem nenhuma imagem anterior disponível, o bootloader é interrompido.
- Na inicialização, o bootloader verifica, conforme descrito anteriormente. Quando a verificação falha sem nenhuma imagem anterior disponível, o carregador de inicialização entra em um modo somente OTA à prova de falhas.
- Um invasor inicializa o dispositivo em uma imagem armazenada anteriormente, que é explorável.

### Exemplos de atenuação

- Os setores flash que armazenam a última imagem são apagados após a instalação e o teste bem-sucedidos de uma nova imagem.
- Um fusível é queimado a cada atualização bem-sucedida, e cada imagem se recusa a ser executada, a menos que o número correto de fusíveis tenha sido queimado.
- Uma atualização OTA fornece uma imagem com falha ou mal-intencionada que bloqueia o dispositivo.

### Exemplo de atenuação

- O bootloader inicia um temporizador de vigilância de hardware que aciona a reversão para a imagem anterior.
- Um invasor corrige o bootloader para ignorar a verificação de imagem para que o dispositivo aceite imagens não assinadas.

### Exemplos de atenuação

- O bootloader está em ROM (memória somente leitura) e não pode ser modificado.



- O bootloader está em OTP (memória programável única) e não pode ser modificado.
- O bootloader está na zona segura do ARM TrustZone e não pode ser modificado.
- Um invasor substitui o certificado de verificação para que o dispositivo aceite imagens mal-intencionadas.

#### Exemplos de atenuação

- O certificado está em um coprocessador criptográfico e não pode ser modificado.
- O certificado está em ROM (ou OTP ou zona segura) e não pode ser modificado.

#### Modelagem adicional de ameaças

Esse modelo de ameaça considera apenas o bootloader. Uma modelagem de ameaças mais ampla pode melhorar a segurança geral. Um método recomendado é listar as metas do adversário, os ativos visados por essas metas e os pontos de entrada dos ativos. Uma lista de ameaças pode ser feita considerando ataques aos pontos de entrada para ganhar controle dos ativos. Veja a seguir listas de exemplos de metas, ativos e pontos de entrada para um dispositivo IoT. Essas listas não são exaustivas e têm como objetivo estimular uma reflexão mais aprofundada.

#### Metas do adversário

- Extorquir dinheiro
- Arruinar reputações
- Falsificar dados
- Desviar recursos
- Espionar remotamente um alvo
- Obter acesso físico a um site
- Causar estragos
- Incutir terror

#### Principais ativos

- Chaves privadas
- Certificado do cliente
- Certificados CA raiz

- Credenciais e tokens de segurança
- Informações de identificação pessoal do cliente
- Implementações de segredos comerciais
- Dados do sensor
- Armazenamento de dados de análise na nuvem
- Infraestrutura de nuvem

#### Pontos de entrada

- Resposta DHCP
- Resposta DNS
- MQTT por TLS
- Resposta HTTPS
- Imagem de software OTA
- Outros, conforme determinado pelo aplicativo, por exemplo, USB
- Acesso físico ao barramento
- IC desanexado

## Portabilidade da biblioteca Cellular Interface

O FreeRTOS oferece suporte aos comandos AT de uma camada de abstração de rede celular descarregada por TCP. Para obter mais informações, consulte a [Biblioteca Cellular Interface](#) e [Fazer portabilidade da biblioteca Cellular Interface](#) em freertos.org.

### Pré-requisitos

Não há dependência direta da biblioteca Cellular Interface. No entanto, na pilha de rede do FreeRTOS, Ethernet, Wi-Fi e rede celular não podem coexistir, então os desenvolvedores devem escolher um deles para integrar com o [Fazer portabilidade da Network Transport Interface](#).

#### Note

Se o módulo de rede celular for compatível com o descarregamento de TLS ou não for compatível com os comandos AT, os desenvolvedores poderão implementar a própria

abstração de rede celular para integração ao [Fazer portabilidade da Network Transport Interface](#).

# Migração do MQTT versão 3 para o coreMQTT

Este [guia de migração](#) explica como migrar aplicativos do MQTT para o coreMQTT.

# Como migrar da versão 1 para a versão 3 para os aplicativos OTA

Este guia ajudará você a migrar sua aplicação da versão 1 da biblioteca OTA para a versão 3.

## Note

As APIs OTA versão 2 são iguais às APIs OTA v3. Portanto, se sua aplicação estiver usando a versão 2 das APIs, as alterações não serão necessárias para as chamadas de API, mas é recomendada a integração da versão 3 da biblioteca.

As demonstrações da versão 3 do OTA estão disponíveis aqui:

- [ota\\_demo\\_core\\_mqtt](#).
- [ota\\_demo\\_core\\_http](#).
- [ota\\_able](#).

## Resumo das alterações da API

Resumo das alterações da API entre a versão 1 e a versão 3 da Biblioteca OTA

API OTA versão 1	API OTA versão 3	Descrição das alterações
OTA_AgentInit	OTA_Init	Os parâmetros de entrada são alterados, assim como o valor retornado da função devido às mudanças na implementação no OTA v3. Consulte a seção <code>OTA_Init</code> abaixo para obter detalhes.
OTA_AgentShutdown	OTA_Shutdown	Alteração nos parâmetros de entrada, incluindo um parâmetro adicional para um cancelamento opcional

API OTA versão 1	API OTA versão 3	Descrição das alterações
		de assinatura dos tópicos do MQTT. Consulte a seção OTA_Shutdown abaixo para obter detalhes.
OTA_GetAgentState	OTA_GetState	O nome da API foi alterado sem alterações no parâmetro de entrada. O valor de retorno é o mesmo, mas o enum e os membros são renomeados. Consulte a seção OTA_GetState abaixo para obter detalhes.
n/a	OTA_GetStatistics	Foram adicionadas novas APIs que substituí as APIs OTA_GetPacketsReceived, OTA_GetPacketsQueued, OTA_GetPacketsProcessed e OTA_GetPacketsDropped. Consulte a seção OTA_GetStatistics abaixo para obter detalhes.
OTA_GetPacketsReceived	n/a	Esta API foi removida da versão 3 e substituída pela OTA_GetStatistics.
OTA_GetPacketsQueued	n/a	Esta API foi removida da versão 3 e substituída pela OTA_GetStatistics.
OTA_GetPacketsProcessed	n/a	Esta API foi removida da versão 3 e substituída pela OTA_GetStatistics.

API OTA versão 1	API OTA versão 3	Descrição das alterações
OTA_GetPacketsDropped	n/a	Esta API foi removida da versão 3 e substituída pela OTA_GetStatistics.
OTA_ActivateNewImage	OTA_ActivateNewImage	Os parâmetros de entrada são os mesmos, mas o código de erro OTA de retorno é renomeado e novos códigos de erro são adicionados na versão 3 da biblioteca OTA. Consulte a seção OTA_ActivateNewImage para obter detalhes.
OTA_SetImageState	OTA_SetImageState	Os parâmetros de entrada são os mesmos e renomeados, o código de erro OTA de retorno é renomeado e novos códigos de erro são adicionados na versão 3 da biblioteca OTA. Consulte a seção OTA_SetImageState para obter detalhes.
OTA_GetImageState	OTA_GetImageState	Os parâmetros de entrada são os mesmos. O enum de retorno é renomeado na versão 3 da biblioteca OTA. Consulte a seção OTA_GetImageState para obter detalhes.

API OTA versão 1	API OTA versão 3	Descrição das alterações
OTA_Suspend	OTA_Suspend	Os parâmetros de entrada são os mesmos, o código de erro OTA de retorno é renomeado e novos códigos de erro são adicionados na versão 3 da biblioteca OTA. Consulte a seção OTA_Suspend para obter detalhes.
OTA_Resume	OTA_Resume	O parâmetro de entrada para a conexão é removido quando a conexão é tratada na demonstração/aplicação OTA, o código de erro OTA de retorno é renomeado e novos códigos de erro são adicionados na versão 3 da biblioteca OTA. Consulte a seção OTA_Resume para obter detalhes.
OTA_CheckForUpdate	OTA_CheckForUpdate	Os parâmetros de entrada são os mesmos, o código de erro OTA de retorno é renomeado e novos códigos de erro são adicionados na versão 3 da biblioteca OTA. Consulte a seção OTA_CheckForUpdate para obter detalhes.



API OTA versão 1	API OTA versão 3	Descrição das alterações
n/a	OTA_EventProcessingTask	Uma nova API foi adicionada e é o principal loop de eventos para lidar com eventos para atualização do OTA e deve ser chamada pela tarefa da aplicação. Consulte a seção OTA_EventProcessingTask para obter detalhes.
n/a	OTA_SignalEvent	Uma nova API foi adicionada e adiciona o evento ao final da fila de eventos OTA e é usada por módulos OTA internos para sinalizar a tarefa do atendente. Consulte a seção OTA_SignalEvent para obter detalhes.
n/a	OTA_Err_streerror	Nova API para conversão de código de erro em string para erros OTA.
n/a	OTA_JobParse_streerror	Nova API para conversão de código de erro em string para erros de Job Parsing.
n/a	OTA_OsStatus_streerror	Nova API para conversão de código de status em string para status de porta do sistema operacional OTA.
n/a	Erro do OTA_PALStatus_STR	Nova API para conversão de código de status em string para status de porta do sistema operacional PAL OTA.

## Descrição das alterações necessárias

### OTA\_Init

Ao inicializar o atendente OTA na v1, a API `OTA_AgentInit` é usada, que usa parâmetros para contexto de conexão, nome da coisa, retorno de chamada completo e tempo limite como entrada.

```
OTA_State_t OTA_AgentInit( void * pvConnectionContext,  
                           const uint8_t * pucThingName,  
                           pxOTACompleteCallback_t xFunc,  
                           TickType_t xTicksToWait );
```

Essa API agora foi alterada para `OTA_Init` com parâmetros para os buffers necessários para ota, interfaces ota, nome da coisa e retorno de chamada da aplicação.

```
OtaErr_t OTA_Init( OtaAppBuffer_t * pOtaBuffer,  
                  OtaInterfaces_t * pOtaInterfaces,  
                  const uint8_t * pThingName,  
                  OtaAppCallback OtaAppCallback );
```

Parâmetros de entrada removidos:

`pvConnectionContext`:

O contexto de conexão é removido porque a Biblioteca OTA Versão 3 não exige que o contexto de conexão seja passado para ela e as operações MQTT/HTTP são tratadas por suas respectivas interfaces na demonstração/aplicação OTA.

`xTicksToWait`:

O parâmetro ticks to wait também é removido quando a tarefa é criada na demonstração/aplicação OTA antes de chamar `OTA_init`.

Parâmetros de entrada renomeados:

`xFunc`:

O parâmetro é renomeado para `OtaAppCallback` e seu tipo é alterado para `OtaAppCallback_t`.

Novos parâmetros de entrada:

`pOtaBuffer`

A aplicação deve alocar os buffers e passá-los para a biblioteca OTA usando a estrutura `OTAAppBuffer_t` durante a inicialização. Os buffers necessários diferem um pouco

dependendo do protocolo usado para baixar o arquivo. Para o protocolo MQTT, os buffers para o nome do fluxo são necessários e, para o protocolo HTTP, os buffers para URL pré-assinado e esquema de autorização são necessários.

Buffers necessários ao usar MQTT para baixar arquivos:

```
static OtaAppBuffer_t otaBuffer =
{
    .pUpdateFilePath      = updateFilePath,
    .updateFilePathsize   = otaexampleMAX_FILE_PATH_SIZE,
    .pCertFilePath       = certFilePath,
    .certFilePathSize    = otaexampleMAX_FILE_PATH_SIZE,
    .pStreamName         = streamName,
    .streamNameSize      = otaexampleMAX_STREAM_NAME_SIZE,
    .pDecodeMemory       = decodeMem,
    .decodeMemorySize    = ( 1U << otaconfigLOG2_FILE_BLOCK_SIZE ),
    .pFileBitmap         = bitmap,
    .fileBitmapSize      = OTA_MAX_BLOCK_BITMAP_SIZE
};
```

Buffers necessários ao usar HTTP para baixar arquivos:

```
static OtaAppBuffer_t otaBuffer =
{
    .pUpdateFilePath      = updateFilePath,
    .updateFilePathsize   = otaexampleMAX_FILE_PATH_SIZE,
    .pCertFilePath       = certFilePath,
    .certFilePathSize    = otaexampleMAX_FILE_PATH_SIZE,
    .pDecodeMemory       = decodeMem,
    .decodeMemorySize    = ( 1U << otaconfigLOG2_FILE_BLOCK_SIZE ),
    .pFileBitmap         = bitmap,
    .fileBitmapSize      = OTA_MAX_BLOCK_BITMAP_SIZE,
    .pUrl                = updateUrl,
    .urlSize              = OTA_MAX_URL_SIZE,
    .pAuthScheme         = authScheme,
    .authSchemeSize      = OTA_MAX_AUTH_SCHEME_SIZE
};
```

Onde:

```
pUpdateFilePath      Path to store the files.
updateFilePathsize   Maximum size of the file path.
```

<code>pCertFilePath</code>	Path to certificate file.
<code>certFilePathSize</code>	Maximum size of the certificate file path.
<code>pStreamName</code>	Name of stream to download the files.
<code>streamNameSize</code>	Maximum size of the stream name.
<code>pDecodeMemory</code>	Place to store the decoded files.
<code>decodeMemorySize</code>	Maximum size of the decoded files buffer.
<code>pFileBitmap</code>	Bitmap of the parameters received.
<code>fileBitmapSize</code>	Maximum size of the bitmap.
<code>pUrl</code>	Presigned url to download files from S3.
<code>urlSize</code>	Maximum size of the URL.
<code>pAuthScheme</code>	Authentication scheme used to validate download.
<code>authSchemeSize</code>	Maximum size of the auth scheme.

## pOtaInterfaces

O segundo parâmetro de entrada para `OTA_Init` é uma referência às interfaces OTA para o tipo `OtaInterfaces_t`. Este conjunto de interfaces deve ser passado para a Biblioteca OTA e inclui na interface do sistema operacional a interface MQTT, a interface HTTP e a interface da camada de abstração da plataforma.

### Interface do sistema operacional OTA

A interface funcional do sistema operacional OTA é um conjunto de APIs que devem ser implementadas para que o dispositivo use a biblioteca OTA. As implementações de funções para essa interface são fornecidas à biblioteca OTA na aplicação do usuário. A biblioteca OTA chama as implementações de funções para executar funcionalidades que normalmente são fornecidas por um sistema operacional. Isto inclui o gerenciamento de eventos, temporizadores e alocação de memória. As implementações para FreeRTOS e POSIX são fornecidas com a biblioteca OTA.

Exemplo para FreeRTOS usando a porta FreeRTOS fornecida:

```
OtaInterfaces_t otaInterfaces;
otaInterfaces.os.event.init    = OtaInitEvent_FreeRTOS;
otaInterfaces.os.event.send   = OtaSendEvent_FreeRTOS;
otaInterfaces.os.event.recv   = OtaReceiveEvent_FreeRTOS;
otaInterfaces.os.event.deinit = OtaDeinitEvent_FreeRTOS;
otaInterfaces.os.timer.start  = OtaStartTimer_FreeRTOS;
otaInterfaces.os.timer.stop   = OtaStopTimer_FreeRTOS;
otaInterfaces.os.timer.delete = OtaDeleteTimer_FreeRTOS;
otaInterfaces.os.mem.malloc   = Malloc_FreeRTOS;
otaInterfaces.os.mem.free     = Free_FreeRTOS;
```

Exemplo para Linux usando a porta POSIX fornecida:

```
OtaInterfaces_t otaInterfaces;
otaInterfaces.os.event.init      = Posix_OtaInitEvent;
otaInterfaces.os.event.send     = Posix_OtaSendEvent;
otaInterfaces.os.event.recv     = Posix_OtaReceiveEvent;
otaInterfaces.os.event.deinit   = Posix_OtaDeinitEvent;
otaInterfaces.os.timer.start    = Posix_OtaStartTimer;
otaInterfaces.os.timer.stop     = Posix_OtaStopTimer;
otaInterfaces.os.timer.delete   = Posix_OtaDeleteTimer;
otaInterfaces.os.mem.malloc     = STDC_Malloc;
otaInterfaces.os.mem.free       = STDC_Free;
```

## Interface MQTT

A interface OTA MQTT é um conjunto de APIs que devem ser implementadas em uma biblioteca para permitir que a biblioteca OTA baixe um bloco de arquivos do serviço de streaming.

Exemplo de uso do atendente coreHTTP da [demonstração OTA por HTTP](#):

```
OtaInterfaces_t otaInterfaces;
otaInterfaces.mqtt.subscribe = prvMqttSubscribe;
otaInterfaces.mqtt.publish  = prvMqttPublish;
otaInterfaces.mqtt.unsubscribe = prvMqttUnSubscribe;
```

## Interface HTTP

A interface HTTP OTA é um conjunto de APIs que devem ser implementadas em uma biblioteca para permitir que a biblioteca OTA baixe um bloco de arquivos conectando-se a um URL pré-assinado e buscando blocos de dados. É opcional, a menos que a biblioteca OTA seja configurada para fazer o download de um URL pré-assinado em vez de um serviço de streaming.

Exemplo de uso das APIs coreHTTP da [demonstração OTA por HTTP](#):

```
OtaInterfaces_t otaInterfaces;
otaInterfaces.http.init = httpInit;
otaInterfaces.http.request = httpRequest;
otaInterfaces.http.deinit = httpDeinit;
```

## Interface PAL OTA

A interface PAL OTA é um conjunto de APIs que devem ser implementadas para que o dispositivo use a biblioteca OTA. A implementação específica do dispositivo para o OTA PAL é fornecida à biblioteca na aplicação do usuário. Estas funções são usadas pela biblioteca para armazenar, gerenciar e autenticar downloads.

```
OtaInterfaces_t otaInterfaces;  
otaInterfaces.pal.getPlatformImageState = otaPal_GetPlatformImageState;  
otaInterfaces.pal.setPlatformImageState = otaPal_SetPlatformImageState;  
otaInterfaces.pal.writeBlock = otaPal_WriteBlock;  
otaInterfaces.pal.activate = otaPal_ActivateNewImage;  
otaInterfaces.pal.closeFile = otaPal_CloseFile;  
otaInterfaces.pal.reset = otaPal_ResetDevice;  
otaInterfaces.pal.abort = otaPal_Abort;  
otaInterfaces.pal.createFile = otaPal_CreateFileForRx;
```

Alterações em retorno:

O retorno é alterado do estado do atendente OTA para o código de erro OTA. Consulte [Atualização do AWS IoT Over-the-Air v3.0.0: Otaerr\\_t](#).

## OTA\_Shutdown

Na versão 1 da Biblioteca OTA, a API usada para desligar o atendente OTA era `OTA_AgentShutdown`, que agora foi alterada para `OTA_Shutdown` junto com as alterações nos parâmetros de entrada.

Desligamento do atendente OTA (versão 1)

```
OTA_State_t OTA_AgentShutdown( TickType_t xTicksToWait );
```

Desligamento do atendente OTA (versão 3)

```
OtaState_t OTA_Shutdown( uint32_t ticksToWait,  
                          uint8_t unsubscribeFlag );
```

`ticksToWait`:

O número de tiques que aguardam até que o atendente OTA conclua o processo de desligamento. Se for definido como zero, a função retornará imediatamente sem esperar. O

estado real é retornado ao chamador. O atendente não fica em repouso nesse tempo, mas é usado para fazer loops ocupados.

Novo parâmetro de entrada:

unsubscribeFlag:

Sinalize para indicar se as operações de cancelamento de assinatura devem ser realizadas nos tópicos do trabalho quando o encerramento é chamado. Se o sinalizador for 0, as operações de cancelamento de inscrição não serão chamadas para tópicos de trabalho. Se a aplicação precisar cancelar a assinatura dos tópicos do trabalho, esse sinalizador deverá ser definido como 1 ao chamar OTA\_Shutdown.

Alterações em retorno:

OtaState\_t:

O enum para o estado do atendente OTA e seus membros é renomeado. Consulte [Atualização do AWS IoT Over-the-Air v3.0.0](#).

## OTA\_GetState

O nome da API foi alterado de OTA\_AgentGetState para OTA\_GetState.

Desligamento do atendente OTA (versão 1)

```
OTA_State_t OTA_GetAgentState( void );
```

Desligamento do atendente OTA (versão 3)

```
OtaState_t OTA_GetState( void );
```

Alterações em retorno:

OtaState\_t:

O enum para o estado do atendente OTA e seus membros é renomeado. Consulte [Atualização do AWS IoT Over-the-Air v3.0.0](#).

## OTA\_GetStatistics

Nova API única adicionada para estatísticas. Ele substitui as APIs `OTA_GetPacketsReceived`, `OTA_GetPacketsQueued`, `OTA_GetPacketsProcessed` e `OTA_GetPacketsDropped`. Além disso, na versão 3 da Biblioteca OTA, os números das estatísticas estão relacionados apenas ao trabalho atual.

### Biblioteca OTA versão 1

```
uint32_t OTA_GetPacketsReceived( void );
uint32_t OTA_GetPacketsQueued( void );
uint32_t OTA_GetPacketsProcessed( void );
uint32_t OTA_GetPacketsDropped( void );
```

### Biblioteca OTA versão 3

```
OtaErr_t OTA_GetStatistics( OtaAgentStatistics_t * pStatistics );
```

`pStatistics`:

O parâmetro de entrada/saída para dados estatísticos, como pacotes recebidos, descartados, colocados em fila e processados para o trabalho atual.

Parâmetro de saída:

Código de erro OTA.

Exemplo de uso:

```
OtaAgentStatistics_t otaStatistics = { 0 };
OTA_GetStatistics( &otaStatistics );
LogInfo( ( " Received: %u   Queued: %u   Processed: %u   Dropped: %u",
          otaStatistics.otaPacketsReceived,
          otaStatistics.otaPacketsQueued,
          otaStatistics.otaPacketsProcessed,
          otaStatistics.otaPacketsDropped ) );
```

## OTA\_ActivateNewImage

Os parâmetros de entrada são os mesmos, mas o código de erro OTA de retorno é renomeado e novos códigos de erro são adicionados na versão 3 da biblioteca OTA.



## Biblioteca OTA versão 1

```
OTA_Err_t OTA_ActivateNewImage( void );
```

## Biblioteca OTA versão 3

```
OtaErr_t OTA_ActivateNewImage( void );
```

A enumeração do código de erro OTA de retorno é alterada e novos códigos de erro são adicionados. Consulte [Atualização do AWS IoT Over-the-Air v3.0.0: Otaerr\\_t](#).

Exemplo de uso:

```
OtaErr_t otaErr = OtaErrNone;
otaErr = OTA_ActivateNewImage();
/* Handle error */
```

## OTA\_SetImageState

Os parâmetros de entrada são os mesmos e renomeados, o código de erro OTA de retorno é renomeado e novos códigos de erro são adicionados na versão 3 da biblioteca OTA.

## Biblioteca OTA versão 1

```
OTA_Err_t OTA_SetImageState( OTA_ImageState_t eState );
```

## Biblioteca OTA versão 3

```
OtaErr_t OTA_SetImageState( OtaImageState_t state );
```

O parâmetro de entrada é renomeado para OtaImageState\_t. Consulte [Atualização do AWS IoT Over-the-Air v3.0.0](#).

A enumeração do código de erro OTA de retorno é alterada e novos códigos de erro são adicionados. Consulte [Atualização do AWS IoT Over-the-Air v3.0.0 /Otaerr\\_t](#).

Exemplo de uso:

```
OtaErr_t otaErr = OtaErrNone;
otaErr = OTA_SetImageState( OtaImageStateAccepted );
```

```
/* Handle error */
```

## OTA\_GetImageState

Os parâmetros de entrada são os mesmos. O enum de retorno é renomeado na versão 3 da biblioteca OTA.

Biblioteca OTA versão 1

```
OTA_ImageState_t OTA_GetImageState( void );
```

Biblioteca OTA versão 3

```
OtaImageState_t OTA_GetImageState( void );
```

A enumeração de retorno é renomeada para `OtaImageState_t`. Consulte [Atualização do AWS IoT Over-the-Air v3.0.0: OtaImageState\\_t](#).

Exemplo de uso:

```
OtaImageState_t imageState;  
imageState = OTA_GetImageState();
```

## OTA\_Suspend

Os parâmetros de entrada são os mesmos, o código de erro OTA de retorno é renomeado e novos códigos de erro são adicionados na versão 3 da biblioteca OTA.

Biblioteca OTA versão 1

```
OTA_Err_t OTA_Suspend( void );
```

Biblioteca OTA versão 3

```
OtaErr_t OTA_Suspend( void );
```

A enumeração do código de erro OTA de retorno é alterada e novos códigos de erro são adicionados. Consulte [Atualização do AWS IoT Over-the-Air v3.0.0: Otaerr\\_t](#).

Exemplo de uso:

```
OtaErr_t xOtaError = OtaErrUninitialized;
xOtaError = OTA_Suspend();
/* Handle error */
```

## OTA\_Resume

O parâmetro de entrada para a conexão é removido quando a conexão é tratada na demonstração/aplicação OTA, o código de erro OTA de retorno é renomeado e novos códigos de erro são adicionados na versão 3 da biblioteca OTA.

Biblioteca OTA versão 1

```
OTA_Err_t OTA_Resume( void * pConnection );
```

Biblioteca OTA versão 3

```
OtaErr_t OTA_Resume( void );
```

A enumeração do código de erro OTA de retorno é alterada e novos códigos de erro são adicionados. Consulte [Atualização do AWS IoT Over-the-Air v3.0.0: Otaerr\\_t](#).

Exemplo de uso:

```
OtaErr_t xOtaError = OtaErrUninitialized;
xOtaError = OTA_Resume();
/* Handle error */
```

## OTA\_CheckForUpdate

Os parâmetros de entrada são os mesmos, o código de erro OTA de retorno é renomeado e novos códigos de erro são adicionados na versão 3 da biblioteca OTA.

Biblioteca OTA versão 1

```
OTA_Err_t OTA_CheckForUpdate( void );
```

## Biblioteca OTA versão 3

```
OtaErr_t OTA_CheckForUpdate( void )
```

A enumeração do código de erro OTA de retorno é alterada e novos códigos de erro são adicionados. Consulte [Atualização do AWS IoT Over-the-Air v3.0.0: Otaerr\\_t](#).

## OTA\_EventProcessingTask

Esta é uma nova API e é o principal loop de eventos para lidar com eventos para atualizações do OTA. Ele deve ser chamado pela tarefa da aplicação. Esse loop continuará manipulando e executando eventos recebidos pela atualização OTA até que essa tarefa seja encerrada pela aplicação.

## Biblioteca OTA versão 3

```
void OTA_EventProcessingTask( void * pUnused );
```

## Exemplo para FreeRTOS:

```
/* Create FreeRTOS task*/
xTaskCreate( prvOTAAgentTask,
            "OTA Agent Task",
            otaexampleAGENT_TASK_STACK_SIZE,
            NULL,
            otaexampleAGENT_TASK_PRIORITY,
            NULL );

/* Call OTA_EventProcessingTask from the task */
static void prvOTAAgentTask( void * pParam )
{
    /* Calling OTA agent task. */
    OTA_EventProcessingTask( pParam );
    LogInfo( ( "OTA Agent stopped." ) );

    /* Delete the task as it is no longer required. */
    vTaskDelete( NULL );
}
```

## Exemplo para POSIX:

```
/* Create posix thread.*/
if( pthread_create( &threadHandle, NULL, otaThread, NULL ) != 0 )
{
    LogError( ( "Failed to create OTA thread: "
                ",errno=%s",
                strerror( errno ) ) );

    /* Handle error. */
}

/* Call OTA_EventProcessingTask from the thread.*/
static void * otaThread( void * pParam )
{
    /* Calling OTA agent task. */
    OTA_EventProcessingTask( pParam );
    LogInfo( ( "OTA Agent stopped." ) );

    return NULL;
}
```

## OTA\_SignalEvent

Esta é uma nova API que adiciona o evento ao final da fila de eventos e também é usada por módulos OTA internos para sinalizar a tarefa do atendente.

### Biblioteca OTA versão 3

```
bool OTA_SignalEvent( const OtaEventMsg_t * const pEventMsg );
```

### Exemplo de uso:

```
OtaEventMsg_t xEventMsg = { 0 };
xEventMsg.eventId = OtaAgentEventStart;
( void ) OTA_SignalEvent( &xEventMsg );
```

# Como integrar a biblioteca OTA como um submódulo em sua aplicação

Se você quiser integrar a biblioteca OTA em sua própria aplicação, você pode usar o comando `git submodule`. Os submódulos Git permitem que você mantenha um repositório Git como um subdiretório de outro repositório Git. A versão 3 da biblioteca OTA é mantida no repositório [ota-for-aws-iot-embedded-sdk](https://github.com/aws/ota-for-aws-iot-embedded-sdk).

```
git submodule add https://github.com/aws/ota-for-aws-iot-embedded-  
sdk.git destination_folder
```

```
git commit -m "Added the OTA Library as submodule to the project."
```

```
git push
```

Para obter mais informações, consulte [Como integrar o atendente OTA em sua aplicação](#) no Manual do usuário do FreeRTOS.

## Referências

- [OTaV1](#).
- [OTaV3](#).

# Migrando da versão 1 para a versão 3 para a porta OTA PAL

A Biblioteca de atualizações sem fios introduziu algumas mudanças na estrutura de pastas e no posicionamento das configurações exigidas pela biblioteca e pelos aplicativos de demonstração. Para que aplicativos OTA projetados para funcionar com a v1.2.0 migrem para a v3.0.0 da biblioteca, você deve atualizar as assinaturas da função da porta PAL e incluir arquivos de configuração adicionais, conforme descrito neste guia de migração.

## Alterações em OTA PAL

- O nome do diretório da porta OTA PAL foi atualizado de `ota_paraota_pal_for_aws`. Essa pasta deve conter dois arquivos: `ota_pal.c` e `ota_pal.h`. O arquivo de cabeçalho PAL `libraries/freertos_plus/aws/ota/src/aws_iot_ota_pal.h` foi excluído da biblioteca OTA e deve ser definido dentro da porta.
- Os códigos de retorno (`OTA_Err_t`) são convertidos em uma enumeração `OTAMainStatus_t`. Consulte [ota\\_platform\\_interface.h](#) para obter os códigos de retorno convertidos. [Macros auxiliares](#) também são fornecidas para combinar os códigos `OtaPalMainStatus` e `OtaPalSubStatus`, e extrair `OtaMainStatus` de `OtaPalStatus` e similares.
- Registro em log na PAL
  - Remova a macro `DEFINE_OTA_METHOD_NAME`.
  - Anteriormente: `OTA_LOG_L1( "[%s] Receive file created.\r\n", OTA_METHOD_NAME );`.
  - Atualizado: use `LogInfo( ( "Receive file created." ) );`, `LogDebug`, `LogWarn` e `LogError` para o log apropriado.
- Variável `cOTA_JSON_FileSignatureKey` alterada para `OTA_JsonFileSignatureKey`.

## Funções

As assinaturas da função são definidas em `ota_pal.h` e começam com o prefixo `otaPal` em vez de `prvPAL`.

**Note**

O nome exato do PAL é tecnicamente aberto, mas para ser compatível com os testes de qualificação, o nome deve estar de acordo com os especificados abaixo.

- Versão 1: `OTA_Err_t prvPAL_CreateFileForRx( OTA_FileContext_t * const *C* );`

Versão 3: `OtaPalStatus_t otaPal_CreateFileForRx( OtaFileContext_t * const *pFileContext* );`

Observações: cria um novo arquivo de recebimento para os blocos de dados à medida que eles chegam.

- Versão 1: `int16_t prvPAL_WriteBlock( OTA_FileContext_t * const C, uint32_t ulOffset, uint8_t * const pData, uint32_t ulBlockSize );`

Versão 3: `int16_t otaPal_WriteBlock( OtaFileContext_t * const pFileContext, uint32_t ulOffset, uint8_t * const pData, uint32_t ulBlockSize );`

Grava um bloco de dados no arquivo especificado no deslocamento determinado.

- Versão 1: `OTA_Err_t prvPAL_ActivateNewImage( void );`

Versão 3: `OtaPalStatus_t otaPal_ActivateNewImage( OtaFileContext_t * const *pFileContext* );`

Observações: ativa a imagem MCU mais recente recebida via OTA.

- Versão 1: `OTA_Err_t prvPAL_ResetDevice( void );`

Versão 3: `OtaPalStatus_t otaPal_ResetDevice( OtaFileContext_t * const *pFileContext* );`

Observações: reinicia o dispositivo.

- Versão 1: `OTA_Err_t prvPAL_CloseFile( OTA_FileContext_t * const *C* );`

Versão 3: `OtaPalStatus_t otaPal_CloseFile( OtaFileContext_t * const *pFileContext* );`



Observações: autentica e fecha o arquivo de recebimento subjacente no contexto OTA especificado.

- Versão 1: `OTA_Err_t prvPAL_Abort( OTA_FileContext_t * const *C* );`

Versão 3: `OtaPalStatus_t otaPal_Abort( OtaFileContext_t * const *pFileContext* );`

Observações: interrompe uma transferência OTA.

- Versão 1: `OTA_Err_t prvPAL_SetPlatformImageState( OTA_ImageState_t *eState* );`

Versão 3: `OtaPalStatus_t otaPal_SetPlatformImageState( OtaFileContext_t * const pFileContext, OtaImageState_t eState );`

Observações: tenta definir o estado da imagem de atualização OTA.

- Versão 1: `OTA_PAL_ImageState_t prvPAL_GetPlatformImageState( void );`

Versão 3: `OtaPalImageState_t otaPal_GetPlatformImageState( OtaFileContext_t * const *pFileContext* );`

Observações: obtém o estado da imagem de atualização OTA.

## Tipos de dados

- Versão 1: `OTA_PAL_ImageState_t`

Arquivo: `aws_iot_ota_agent.h`

Versão 3: `OtaPalImageState_t`

Arquivo: `ota_private.h`

Observações: o estado da imagem definido pela implementação da plataforma.

- Versão 1: `OTA_Err_t`

Arquivo: `aws_iot_ota_agent.h`

Versão 3: `OtaErr_t OtaPalStatus_t` (combination of `OtaPalMainStatus_t` and `OtaPalSubStatus_t`)

Arquivo `ota.h`, `ota_platform_interface.h`

Observações: v1: esses macros definiam um número inteiro de 32 não assinado. v3: enumeração especializada representando o tipo de erro e associada a um código de erro.

- Versão 1: `OTA_FileContext_t`

Arquivo: `aws_iot_ota_agent.h`

Versão 3: `OtaFileContext_t`

Arquivo: `ota_private.h`

Observações: v1: contém uma enumeração e buffers para os dados. v3: contém variáveis adicionais de comprimento de dados.

- Versão 1: `OTA_ImageState_t`

Arquivo: `aws_iot_ota_agent.h`

Versão 3: `OtaImageState_t`

Arquivo: `ota_private.h`

Observações: estados de imagem OTA

## Alterações de configuração

O arquivo `aws_ota_agent_config.h` foi renomeado para [ota\\_config.h](#), o que altera as guards incluídos de `_AWS_OTA_AGENT_CONFIG_H_` para `OTA_CONFIG_H_`.

- O arquivo `aws_ota_codesigner_certificate.h` foi excluído.
- Incluiu a nova pilha de registro em log para imprimir mensagens de depuração:

```
/*
*****
***** DO NOT CHANGE the following order *****
*****
*/

/* Logging related header files are required to be included in the following order:
 * 1. Include the header file "logging_levels.h".
 * 2. Define LIBRARY_LOG_NAME and LIBRARY_LOG_LEVEL.
 * 3. Include the header file "logging_stack.h".
*/
```

```

*/

/* Include header that defines log levels. */
#include "logging_levels.h"

/* Configure name and log level for the OTA library. */
#ifndef LIBRARY_LOG_NAME
    #define LIBRARY_LOG_NAME    "OTA"
#endif
#ifndef LIBRARY_LOG_LEVEL
    #define LIBRARY_LOG_LEVEL    LOG_INFO
#endif

#include "logging_stack.h"

/***** End of logging configuration *****/

```

- Configuração constante adicionada:

```

/** * @brief Size of the file data block message (excluding the header). */
#define otaconfigFILE_BLOCK_SIZE ( 1UL << otaconfigLOG2_FILE_BLOCK_SIZE )

```

Novo arquivo: [ota\\_demo\\_config.h](#) contém as configurações exigidas pela demonstração OTA, como o certificado de assinatura de código e a versão do aplicativo.

- `signingcredentialSIGNING_CERTIFICATE_PEM` que foi definido em `demos/include/aws_ota_codesigner_certificate.h` foi movido para `ota_demo_config.h` as `otapalconfigCODE_SIGNING_CERTIFICATE` e pode ser acessado a partir dos arquivos PAL como:

```

static const char codeSigningCertificatePEM[] = otapalconfigCODE_SIGNING_CERTIFICATE;

```

O arquivo `aws_ota_codesigner_certificate.h` foi excluído.

- As macros `APP_VERSION_BUILD`, `APP_VERSION_MINOR`, `APP_VERSION_MAJOR` foram adicionadas a `ota_demo_config.h`. Os arquivos antigos contendo as informações da versão foram removidos, por exemplo `tests/include/aws_application_version.h`, `libraries/c_sdk/standard/common/include/iot_appversion32.h`, `demos/demo_runner/aws_demo_version.c`.

## Alterações nos testes OTA PAL

- O grupo de teste "FULL\_OTA\_Agent" foi removido junto com todos os arquivos relacionados. Esse grupo de teste era exigido anteriormente para qualificação. Esses testes foram para a biblioteca OTA e não específicos para a porta OTA PAL. A biblioteca OTA agora tem cobertura de teste completa hospedada no repositório OTA, portanto, esse grupo de teste não é mais necessário.
- Os grupos de teste "Full\_OTA\_CBOR" e "Quarantine\_OTA\_CBOR" foram removidos, bem como todos os arquivos relacionados. Esses testes não faziam parte dos testes de qualificação. As funcionalidades abordadas por esses testes agora estão sendo testadas no repositório OTA.
- Os arquivos de teste foram movidos do diretório da biblioteca para o diretório `tests/integration_tests/ota_pal`.
- Os testes de qualificação OTA PAL foram atualizados para usar a versão 3.0.0 da API da biblioteca OTA.
- A forma como os testes OTA PAL acessam o certificado de assinatura de código para testes foi atualizada. Anteriormente, havia um arquivo de cabeçalho dedicado para a credencial de assinatura de código. Esse não é mais o caso da nova versão da biblioteca. O código de teste espera que essa variável seja definida em `ota_pal.c`. O valor é atribuído a uma macro definida no arquivo de configuração OTA específico da plataforma.

## Lista de verificação

Use essa lista de verificação para seguir as etapas necessárias para a migração:

- Atualize o nome da pasta da porta OTA PAL de `ota` para `ota_pal_for_aws`.
- Adicione o arquivo `ota_pal.h` com as funções mencionadas acima. Para ver um exemplo de arquivo `ota_pal.h`, consulte [GitHub](#).
- Adicione os arquivos de configuração:
  - Altere o nome do arquivo de `aws_ota_agent_config.h` para (ou crie) `ota_config.h`.
  - Adicionar:

```
otaconfigFILE_BLOCK_SIZE ( 1UL << otaconfigLOG2_FILE_BLOCK_SIZE )
```

- Inclusão:

```
#include "ota_demo_config.h"
```

- Copie os arquivos acima para a pasta `aws_test_config` e substitua as inclusões de `ota_demo_config.h` por `aws_test_ota_config.h`.
- Adicione um arquivo `ota_demo_config.h`.
- Adicione um arquivo `aws_test_ota_config.h`.
- Faça as seguintes alterações em `ota_pal.c`:
  - Atualize as inclusões com os nomes mais recentes dos arquivos da biblioteca OTA.
  - Remova a macro `DEFINE_OTA_METHOD_NAME`.
  - Atualize as assinaturas das funções OTA PAL.
  - Atualize o nome da variável de contexto do arquivo de C para `pFileContext`.
  - Atualize a estrutura `OTA_FileContext_t` e todas as variáveis relacionadas.
  - Atualize `cOTA_JSON_FileSignatureKey` para `OTA_JsonFileSignatureKey`.
  - Atualize os tipos `OTA_PAL_ImageState_t` e `Ota_ImageState_t`.
  - Atualize o tipo de erro e os valores.
  - Atualize as macros de impressão para usar a pilha de registro em log.
  - Atualize o `signingcredentialSIGNING_CERTIFICATE_PEM` para ser `otapalconfigCODE_SIGNING_CERTIFICATE`.
  - Atualize os comentários de função `otaPal_CheckFileSignature` e `otaPal_ReadAndAssumeCertificate`.
- Para atualizar o arquivo [CMakeLists.txt](#).
- Atualize os projetos do IDE.

## Histórico do documentos

A tabela a seguir descreve o histórico da documentação do Guia de portabilidade do FreeRTOS e do Guia de qualificação do FreeRTOS.

Data	Versão da documentação	Histórico de alterações	Versão do FreeRTOS
Maio de 2022	<a href="#">Guia de portabilidade do FreeRTOS</a> <a href="#">Guia de qualificação do FreeRTOS</a>	<ul style="list-style-type: none"> <li>• Atualizou os testes existentes, adicionou novos testes e removeu testes redundantes com base nas Bibliotecas de suporte de longo prazo (LTS) do FreeRTOS. Para obter mais informações, consulte Testes de integração das bibliotecas do FreeRTOS <a href="#">202205.00</a> no GitHub.</li> <li>• Atualizado <a href="#">Fluxograma de portabilidade do FreeRTOS</a>.</li> <li>• Adicionou um novo <a href="#">Fazer portabilidade da Network Transport Interface</a>.</li> </ul>	<a href="#">202012.04-LTS</a> <a href="#">202112.00</a>

Data	Versão da documentação	Histórico de alterações	Versão do FreeRTOS
		<ul style="list-style-type: none"><li>• Agora, <a href="#">Portabilidade da biblioteca de atualização sem fios do AWS IoT</a> é necessário para a qualificação.</li><li>• Guia de portabilidade de abstração de Wi-Fi e TLS removido, pois ele não é mais necessário.</li><li>• Consulte as <a href="#">últimas mudanças</a> para obter mais atualizações sobre a qualificação dos FreeRTOS.</li></ul>	

Data	Versão da documentação	Histórico de alterações	Versão do FreeRTOS
Julho de 2022	<a href="#">202107.00</a> (Guia de portabilidade) <a href="#">202107.00</a> (Guia de qualificação)	<ul style="list-style-type: none"> <li>Versão 202107.00</li> <li><a href="#">Portabilidade da biblioteca de atualização sem fios do AWS IoT</a> alterado</li> <li>Adicionado <a href="#">Como migrar da versão 1 para a versão 3 para os aplicativos OTA</a></li> <li>Adicionado <a href="#">Migrando da versão 1 para a versão 3 para a porta OTA PAL</a></li> </ul>	<a href="#">202107.00</a>
Dezembro de 2020	<a href="#">202012.00</a> (Guia de portabilidade) <a href="#">202002.00</a> (Guia de qualificação)	<ul style="list-style-type: none"> <li>Versão 202012.00</li> <li>Adicionado <a href="#">Configuração da biblioteca coreHTTP</a></li> <li>Adicionado <a href="#">Portabilidade da biblioteca Cellular Interface</a></li> </ul>	<a href="#">202012.00</a>
Novembro de 2020	<a href="#">202011.00</a> (Guia de portabilidade) <a href="#">202011.00</a> (Guia de qualificação)	<ul style="list-style-type: none"> <li>Versão 202011.00</li> <li>Adicionado <a href="#">Configuração da biblioteca coreMQTT</a></li> </ul>	<a href="#">202011.00</a>



Data	Versão da documentação	Histórico de alterações	Versão do FreeRTOS
Julho de 2020	<a href="#">202007.00</a> (Guia de portabilidade) <a href="#">202007.00</a> (Guia de qualificação)	<ul style="list-style-type: none"> <li>Versão 202007.00</li> </ul>	<a href="#">202007.00</a>
18 de fevereiro de 2020	<a href="#">202002.00</a> (Guia de transferência) <a href="#">202002.00</a> (Guia de qualificação)	<ul style="list-style-type: none"> <li>Versão 202002.00</li> <li>Agora, o Amazon FreeRTOS é FreeRTOS</li> </ul>	<a href="#">202002.00</a>
17 de dezembro de 2019	<a href="#">201912.00</a> (Guia de transferência) <a href="#">201912.00</a> (Guia de qualificação)	<ul style="list-style-type: none"> <li>Versão 201912.00</li> <li>Portabilidade das bibliotecas de E/S comuns adicionada.</li> </ul>	<a href="#">201912.00</a>
29 de outubro de 2019	<a href="#">201910.00</a> (Guia de transferência) <a href="#">201910.00</a> (Guia de qualificação)	<ul style="list-style-type: none"> <li>Versão 201910.00</li> <li>Atualização das informações sobre portabilidade do gerador de números aleatórios.</li> </ul>	<a href="#">201910.00</a>
26 de agosto de 2019	<a href="#">201908.00</a> (Guia de transferência) <a href="#">201908.00</a> (Guia de qualificação)	<ul style="list-style-type: none"> <li>Versão 201908.00</li> <li>Configuração da biblioteca de cliente HTTPS para testes adicionada</li> </ul> <p>Atualização do <a href="#">Portabilidade da biblioteca corePKCS11</a></p>	<a href="#">201908.00</a>

Data	Versão da documentação	Histórico de alterações	Versão do FreeRTOS
17 de junho de 2019	<a href="#">201906.00</a> (Guia de portabilidade) <a href="#">201906.00</a> (Guia de qualificação)	<ul style="list-style-type: none"> <li>Versão 201906.00</li> <li>Diretório estrutura do atualizado</li> </ul>	<a href="#">201906.00 principal</a>
21 de maio de 2019	<a href="#">1.4.8</a> (Guia de portabilidade) <a href="#">1.4.8</a> (Guia de qualificação)	<ul style="list-style-type: none"> <li>Documentação de portabilidade movida para o <a href="#">Guia de portabilidade do FreeRTOS</a></li> <li>Documentação de qualificação movida para o <a href="#">Guia de qualificação do FreeRTOS</a></li> </ul>	<a href="#">1.4.8</a>
25 de fevereiro de 2019	<a href="#">1.1.6</a>	<ul style="list-style-type: none"> <li>Instruções de download e configuração removidas do Apêndice Modelo do guia de conceitos básicos (página 84)</li> </ul>	<a href="#">1.4.5</a> <a href="#">1.4.6</a> <a href="#">1.4.7</a>
27 de dezembro de 2018	<a href="#">1.1.5</a>	<ul style="list-style-type: none"> <li>Apêndice Lista de verificação para qualificação atualizado com o requisito do CMake (página 70)</li> </ul>	<a href="#">1.4.5</a> <a href="#">1.4.6</a>

Data	Versão da documentação	Histórico de alterações	Versão do FreeRTOS
12 de dezembro de 2018	<a href="#">1.1.4</a>	<ul style="list-style-type: none"><li>• Instruções de portabilidade lwIP adicionadas ao apêndice Portabilidade TCP/IP (página 31)</li></ul>	<a href="#">1.4.5</a>
26 de novembro de 2018	<a href="#">1.1.3</a>	<ul style="list-style-type: none"><li>• Inclusão do apêndice de portabilidade da biblioteca Bluetooth Low Energy (página 52)</li><li>• AWS IoT Device Tester adicionado para informações de teste do FreeRTOS em todo o documento</li><li>• Link do CMake adicionado em Informações para listagem no apêndice Console do FreeRTOS (página 85)</li></ul>	<a href="#">1.4.4</a>

Data	Versão da documentação	Histórico de alterações	Versão do FreeRTOS
7 de novembro de 2018	<a href="#">1.1.2</a>	<ul style="list-style-type: none"><li>• Instruções de portabilidade da interface PAL PKCS #11 atualizadas no apêndice de portabilidade PKCS #11 (página 38)</li><li>• Caminho atualizado para CertificateConfigurator.html (página 76)</li><li>• Apêndice Modelo do guia de conceitos básicos atualizado (página 80)</li></ul>	<a href="#">1.4.3</a>

Data	Versão da documentação	Histórico de alterações	Versão do FreeRTOS
8 de outubro de 2018	<a href="#">1.1.1</a>	<ul style="list-style-type: none"><li>• Nova coluna "Necessário para AFQP" para <code>aws_test_runner_config.h</code> testar a tabela de configuração (página 16)</li><li>• Caminho do diretório do módulo do Unity atualizado na seção Criar o projeto de teste (página 14)</li><li>• Gráfico "Ordem de portabilidade recomendada" atualizado (página 22)</li><li>• Certificado de cliente e nomes de variáveis de chave atualizados no apêndice TLS, Configuração de teste (página 40)</li><li>• Caminhos de arquivo alterados no apêndice Portabilidade de Secure Sockets, Configuração de teste (página 34);</li></ul>	<a href="#">1.4.2</a>

Data	Versão da documentação	Histórico de alterações	Versão do FreeRTOS
		apêndice Portabilidade do TLS, Configuração de teste (página 40); e apêndice Configuração do servidor TLS (página 57)	
27 de agosto de 2018	<a href="#">1.1.0</a>	<ul style="list-style-type: none"><li>• Apêndice Portabilidade das atualizações OTA adicionado (página 47)</li><li>• Apêndice Portabilidade do bootloader adicionado (página 51)</li></ul>	<a href="#">1.4.0</a> <a href="#">1.4.1</a>

Data	Versão da documentação	Histórico de alterações	Versão do FreeRTOS
9 de agosto de 2018	<a href="#">1.0.1</a>	<ul style="list-style-type: none"><li>• Gráfico "Ordem de portabilidade recomendada" atualizado (página 22)</li><li>• Apêndice Portabilidade PKCS #11 atualizado (página 36)</li><li>• Caminhos de arquivo alterados no apêndice Portabilidade do TLS, Configuração de teste (página 40) e apêndice Configuração do servidor TLS, etapa 9 (página 51)</li><li>• Hiperlinks corrigidos no apêndice Portabilidade MQTT, Pré-requisitos (página 45)</li><li>• Instruções de configuração da AWS CLI adicionadas aos exemplos no apêndice Instruções para criar um BYOC (página 57)</li></ul>	<a href="#">1.3.1</a> <a href="#">1.3.2</a>

Data	Versão da documentação	Histórico de alterações	Versão do FreeRTOS
31 de julho de 2018	<a href="#">1.0.0</a>	Versão inicial do Guia do programa de qualificação do FreeRTOS	<a href="#">1.3.0</a>



As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.