Host Security Service

Visão geral de serviço

Edição 01

Data 2023-10-27

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Marcas registadas e permissões

e outras marcas registadas da Huawei são marcas registadas da Huawei Technologies Co., Ltd. Todos as outras marcas registadas e os nomes registados mencionados neste documento são propriedade dos seus respectivos detentores.

Aviso

Os produtos, os serviços e as funcionalidades adquiridos são estipulados pelo contrato estabelecido entre a Huawei Cloud e o cliente. Os produtos, os serviços e as funcionalidades descritos neste documento, no todo ou em parte, podem não estar dentro do âmbito de aquisição ou do âmbito de uso. Salvo especificação em contrário no contrato, todas as declarações, informações e recomendações neste documento são fornecidas "TAL COMO ESTÃO" sem garantias ou representações de qualquer tipo, sejam expressas ou implícitas.

As informações contidas neste documento estão sujeitas a alterações sem aviso prévio. Foram feitos todos os esforços na preparação deste documento para assegurar a exatidão do conteúdo, mas todas as declarações, informações e recomendações contidas neste documento não constituem uma garantia de qualquer tipo, expressa ou implícita.

Huawei Cloud Computing Technologies Co., Ltd.

Endereço: Huawei Cloud Data Center, Rua Jiaoxinggong
Avenida Qianzhong
Novo Distrito de Gui'an
Guizhou 550029
República Popular da China

Site: https://www.huaweicloud.com/intl/pt-br/

Índice

1 O que é o HSS?

O Host Security Service (HSS) foi projetado para proteger cargas de trabalho de servidor em nuvens híbridas e data centers multinuvem. Ele fornece funções de segurança de host, Container Guard Service (CGS) e Proteção contra adulterações na Web (WTP).

O HSS pode ajudá-lo a verificar e gerenciar remotamente seus servidores e containers de maneira unificada.

O HSS protege a integridade do sistema, aumenta a segurança da aplicação, monitora as operações do usuário e detecta invasões.

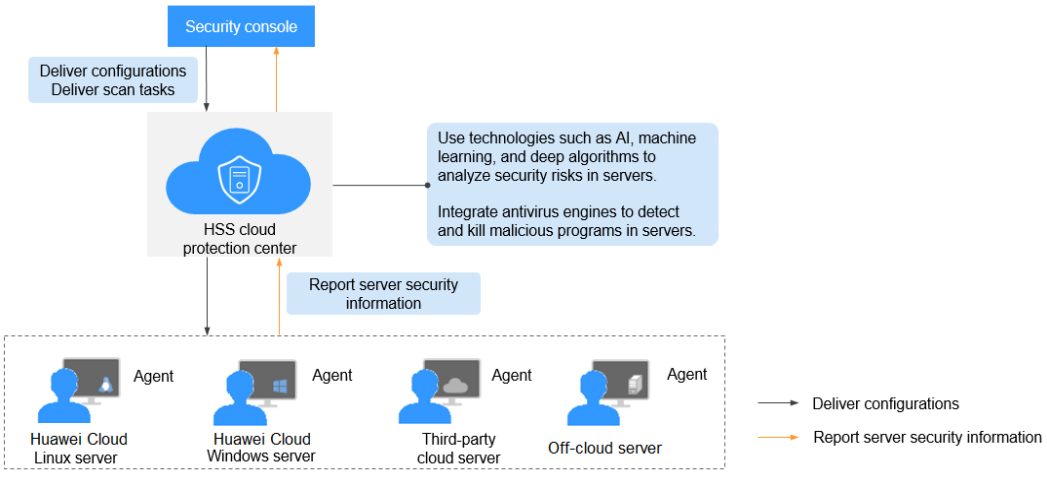
Segurança do host

O Host Security Service (HSS) ajuda você a identificar e gerenciar os ativos em seus servidores, eliminar riscos e defender-se contra invasões e adulteração de páginas da Web. Há também funções avançadas de proteção e operações de segurança disponíveis para ajudá-lo a detectar e lidar facilmente com as ameaças.

Instale o agente do HSS em seus servidores e você poderá verificar o status da proteção do servidor e os riscos em uma região no console do HSS.

Figura 1-1 ilustra como funciona o HSS.

Figura 1-1 Princípios de funcionamento



A tabela a seguir descreve os componentes do HSS.

Tabela 1-1 Componentes

Componente	Descrição
Console de gerenciamento	Uma plataforma de gerenciamento visualizada, onde você pode aplicar configurações de maneira centralizada e visualizar o status de proteção e os resultados da verificação de servidores em uma região.
Centro de proteção em nuvem de HSS	● Analisa os riscos de segurança em servidores usando IA, aprendizado de máquina e algoritmos de aprendizado profundo. ● Integra vários mecanismos antivírus para detectar e eliminar programas maliciosos em servidores. ● Recebe configurações e tarefas de verificação enviadas do console e as encaminha para agentes nos servidores. ● Recebe informações do servidor relatadas pelos agentes, analisa os riscos de segurança e exceções nos servidores e exibe os resultados da análise no console.
Agente	● Comunica-se com o centro de proteção em nuvem de HSS via HTTPS e WSS. A porta 10180 é usada por padrão. ● Verifica todos os servidores todas as manhãs; monitora o status de segurança dos servidores; e relata as informações coletadas do servidor (incluindo configurações não compatíveis, configurações inseguras, rastreamentos de intrusão, lista de software, lista de portas e lista de processos) para o centro de proteção em nuvem. ● Bloqueia ataques ao servidor com base nas políticas de segurança que você configurou. **NOTA** ● Se nenhum agente for instalado ou se o agente instalado for anormal, o HSS não estará disponível. ● O agente pode ser instalado em Elastic Cloud Servers (ECSs) e Bare Metal Servers (BMSs) da Huawei Cloud, servidores locais e servidores de nuvem de terceiros. ● Selecione o agente e o comando de instalação adequados para o seu SO. ● O agente do HSS pode ser usado em todas as edições, incluindo segurança de container e Proteção contra adulterações na Web (WTP). Você só precisa instalar o agente uma vez no mesmo servidor.

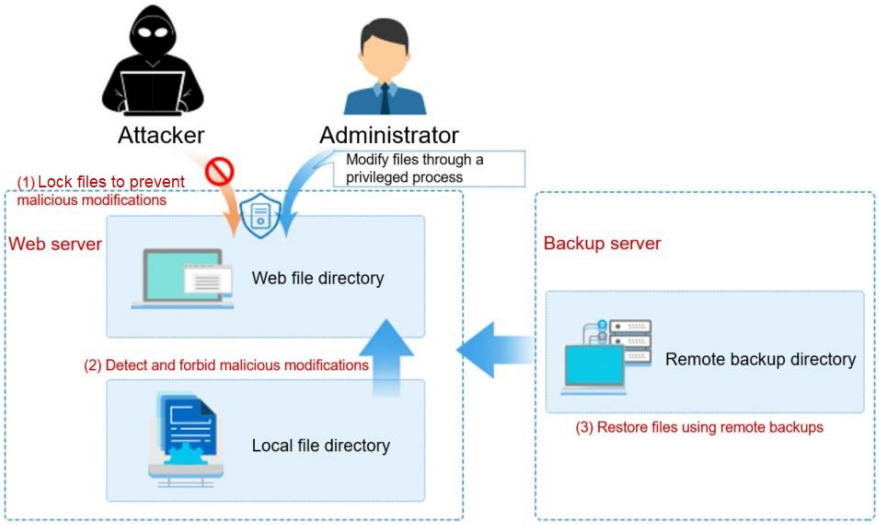
Segurança de containers

O HSS fornece recursos de segurança de containers. O agente implementado em um servidor pode verificar as imagens de containers no servidor, verificar configurações, detectar vulnerabilidades e descobrir problemas de tempo de execução que não podem ser detectados pelo software de segurança tradicional. A segurança de container também fornece funções como lista branca de processos, proteção de arquivos somente leitura e detecção de escape de container para minimizar os riscos de segurança de um container em execução.

Proteção contra adulteração na Web

Proteção contra adulteração na Web (WTP) monitora diretórios de sites em tempo real e restaura arquivos e diretórios adulterados usando seus backups. Ela protege as informações do site, como páginas da Web, documentos eletrônicos e imagens, de serem adulteradas ou danificadas por hackers.

Figura 1-2 Como funciona a WTP



2 Vantagens

O HSS ajuda você a gerenciar e manter a segurança de todos os seus servidores e reduzir os riscos comuns.

Gerenciamento centralizado

Você pode verificar e corrigir uma série de problemas de segurança em um único console, gerenciando facilmente seus servidores.

- Você pode instalar o agente em ECSs, BMSs, servidores locais e servidores de nuvem de terceiros da Huawei Cloud na mesma região para gerenciar todos eles em um único console.
- No console de segurança, você pode visualizar as origens dos riscos de servidor em uma região, tratá-las de acordo com as sugestões exibidas e usar as funções de filtro, pesquisa e processamento em lote para analisar rapidamente os riscos de todos os servidores na região.

Defesa precisa

O HSS bloqueia ataques com precisão exata, usando tecnologias avançadas de detecção e diversas bibliotecas.

Proteção completa

O HSS protege os servidores contra invasões por meio de prevenção, defesa e verificação pós-intrusão.

Agente leve

O agente ocupa apenas alguns recursos, não afetando o desempenho do sistema do servidor.

WTP

- A tecnologia anti-adulteração da Web de terceira geração e a tecnologia de acionamento de eventos no nível do kernel são usadas. Arquivos em diretórios de usuário podem ser bloqueados para evitar adulteração não autorizada.
- As tecnologias de detecção e recuperação de adulteração são usadas. Os arquivos modificados apenas por usuários autorizados têm backup em servidores locais e remotos

em tempo real e serão usadospara recuperar sites adulterados (se houver) detectados pelo HSS.

3 Edições e recursos

O HSS está disponível nas edições básica, profissional, empresarial, premium, WTP (Proteção contra adulteração na Web) e de containers, fornecendo gerenciamento de ativos, gerenciamento de vulnerabilidades, verificação de linha de base, detecção de intrusão, proteção contra ransomware, proteção contra adulteração na Web e funções de segurança de imagem de container. Para obter detalhes sobre os recursos das edições, consulte **Detalhes da edição**.

AVISO

- O HSS está disponível nas edições básica, profissional, empresarial, premium, WTP (Proteção contra adulteração na Web) e container. Você pode comprar ou atualizar sua edição conforme necessário.

  Você pode atualizar suas edições nos seguintes cenários.

  - Se você comprou a edição básica anual/mensal, poderá atualizá-la para a edição empresarial, profissional ou premium. Para usar a WTP ou a edição de container, você precisa cancelar a assinatura da edição básica e, em seguida, comprar e ativar a edição de destino.
  - Se você comprou a edição profissional anual/mensal, pode atualizá-la para a edição empresarial ou premium. Para usar a edição WTP ou de container, você precisa cancelar a assinatura da edição profissional e, em seguida, comprar e ativar a edição de destino.
  - Se você tiver comprado a edição empresarial anual/mensal, poderá atualizá-la para a edição premium. Para usar a WTP ou a edição de container, você precisa cancelar a assinatura da edição empresarial e, em seguida, comprar e ativar a edição de destino.
- A edição premium é fornecida gratuitamente se você tiver comprado a edição WTP.

Recursos

O HSS fornece recursos de gerenciamento de ativos, verificação de linha de base, prevenção contra ransomware e detecção de intrusões, aprimorando a segurança do servidor em todos os aspectos. Para obter detalhes sobre os recursos de diferentes edições, consulte **Detalhes da edição**.

Tabela 3-1 Recursos do HSS

Recurso	Descrição
Gerenciamento de ativos	Fornecer uma visão geral centralizada de ativos, gerenciamento de impressões digitais de ativos, gerenciamento de servidores e gerenciamento de containers. Você pode verificar seu status de execução de ativos, impressões digitais de ativos e tipos de ativos; e gerenciar ativos por servidor ou container.
Gerenciamento de vulnerabilidades	Detectar vulnerabilidades e riscos em Linux, Windows, sistemas de gerenciamento de conteúdo da Web (Web-CMS) e aplicações.
Verificação da linha de base	Procurar configurações inseguras, senhas fracas e políticas de complexidade de senha no SO do servidor e no software de chave. Uma linha de base de práticas de segurança e uma linha de base padrão de conformidade podem ser usadas para verificações. Você pode personalizar os subitens da linha de base usados na verificação. Você pode reparar e verificar os riscos detectados.
Segurança de imagens de containers	Verificar as imagens que estão em execução ou exibidas na sua lista de imagens e fornecer sugestões sobre como corrigir vulnerabilidades e arquivos maliciosos.
Proteção da aplicação	Proteger aplicações em execução. Você simplesmente precisa adicionar sondas às aplicações, sem ter que modificar os arquivos da aplicação. Atualmente, apenas servidores de Linux são suportados e apenas aplicações Java podem ser conectadas.
Prevenção de adulteração na páginas da Web	Detectar e impedir a adulteração de arquivos em diretórios específicos, incluindo páginas da Web, documentos e imagens, e restaurá-los rapidamente usando arquivos de backup válidos.
Prevenção contra ransomware	Detectar ransomware conhecido e oferecer suporte a políticas de backup e restauração de ransomware definidas pelo usuário.
Monitoramento da integridade de arquivos	Verificar os arquivos no SO Linux, aplicações e outros componentes para detectar adulteração.

Recurso	Descrição
Controle de processo de aplicação	Controlar diferentes tipos de processos de aplicação em servidores. Processos suspeitos e confiáveis podem ser executados, e alarmes são gerados para processos maliciosos.
Firewall de container	Controlar e interceptar o tráfego de rede dentro e fora de um cluster de containers para evitar acesso e ataques maliciosos.
Proteção de cluster de containers	Verificar se há problemas de linha de base de não conformidade, vulnerabilidades e arquivos maliciosos quando uma imagem de container é iniciada e relatar alarmes ou bloquear a inicialização do container que não tenha sido não autorizada ou possa incorrer em altos riscos.
Detecção de intrusão	Identificar e impedir a intrusão em servidores, descobrir riscos em tempo real, detectar e eliminar programas maliciosos e identificar web shells e outras ameaças.
Detecção de intrusão de container	Verificar containers em execução em busca de programas maliciosos, incluindo mineradores e ransomware; detectar políticas de segurança não compatíveis, adulteração de arquivos e escape de containers; e fornecer sugestões.
Gerenciamento de listas brancas	Para reduzir alarmes falsos, importar e exportar eventos da lista branca. Os eventos na lista branca não acionarão alarmes.
Gerenciamento de políticas	Você pode agrupar políticas e servidores para aplicar políticas em lote a servidores, adaptando-se facilmente a seus cenários de negócios.
Histórico de manipulação	Verificar o histórico de vulnerabilidades e registros de manipulação de alarmes, incluindo o tempo de manipulação e manipuladores.
Relatório de segurança	Verificar semanalmente ou mensalmente as tendências de segurança do servidor, os principais eventos de segurança e os riscos.
Configuração de segurança	Configurar localizações de logon comuns, endereços IP de logon comuns, a lista branca de endereços IP de logon SSH e o isolamento e eliminação automáticos de programas maliciosos.
Autoproteção do HSS	Proteger arquivos, processos e softwares do HSS contra programas maliciosos, que podem desinstalar agentes do HSS, adulterar arquivos do HSS ou interromper processos do HSS.

Para obter detalhes sobre alarmes de vulnerabilidade, consulte **Gerenciamento de vulnerabilidades**.

Para obter detalhes sobre alarmes de risco de ativos, consulte **Verificação de linha de base**.

Para obter detalhes sobre vulnerabilidades e alarmes de imagem de container, consulte **Verificação da segurança da imagem de container**.

Para obter detalhes sobre alarmes de proteção de servidor e container, consulte **Alarmes**.

Edições recomendadas

- Para proteger servidores de teste ou servidores de usuários individuais, use a edição básica. Ela pode proteger qualquer número de servidores, mas apenas parte dos recursos de verificação de segurança estão disponíveis. Esta edição não fornece recursos de proteção, nem fornece suporte para a certificação DJCP Multi-level Protection Scheme (MLPS). Para um servidor que usa a edição básica pela primeira vez, esta edição é gratuita por 30 dias.
- Se você precisar obter a certificação DJCP MLPS L2, compre a edição empresarial. Se você precisa obter a certificação DJCP MLPS L3, compre a edição premium. Se você precisa obter a certificação DJCP MLPS para um site, compre a edição de Proteção contra adulteração na Web.
- Se seus servidores armazenam ativos de dados importantes, têm altos riscos de segurança, usam EIPs disponíveis publicamente ou há bancos de dados em execução em seus servidores, você é aconselhado a ativar a edição premium ou de Proteção contra adulteração na Web.
- Para servidores que precisam proteger sites e aplicações contra adulteração, recomenda-se a edição WTP.
- Para containers que precisam aprimorar a segurança da imagem, a segurança do tempo de execução do container e para estar em conformidade com os regulamentos de segurança, a edição de container é recomendada.

AVISO

- É aconselhável implementar o HSS em todos os seus servidores para que, se um vírus infectar um deles, ele não possa se espalhar para outros e danificar toda a sua rede.
- No modo **Pay-per-use**, a edição empresarial do HSS pára de cobrar se os servidores que protege são interrompidos.

Detalhes da edição

Tabela 3-2 Edições

Função	Item	Descrição	Edição básica	Edição profissional	Edição empresarial	Edição premium	Edição WTP	Edição de container	SO suportado	Frequência de verificação
Ativos		Coletar estatísticas sobre o status dos ativos e o uso de todos os servidores.	√	√	√	√	√	√	Linux e Windows	Verificação em tempo real
Servidores e cotas		Gerenciar todos os ativos do servidor, incluindo seus status de proteção, cotas e políticas. Você pode instalar agentes em todos os servidores de Linux em lotes.	√	√	√	√	√	√	Linux e Windows Observação: somente agentes do Linux podem ser instalados em lotes.	-
Containers e cota		Gerenciar nós e imagens de contêiner (repositórios de imagens privadas e imagens locais).	×	×	×	×	×	√	Linux	-

Função	Item	Descrição	Edição básica	Edição profissional	Edição empresarial	Edição premium	Edição WTP	Edição de container	SO suportado	Frequência de verificação
Impressões digitais de ativos	Conta	Verificar e gerenciar contas de servidor em um só lugar.	×	×	√	√	√	√	Linux e Windows	Verificação em tempo real
	Porta aberta	Verificar as portas abertas em um só lugar e identificar portas desconhecidas e de alto risco.	×	×	√	√	√	√	Linux e Windows	Verificação em tempo real
	Processo	Verificar as aplicações em execução em um só lugar e identificar aplicações maliciosas.	×	×	√	√	√	√	Linux e Windows	Verificação em tempo real
	Software instalado	Verificar e gerenciar o software do servidor em um só lugar e identificar versões inseguras.	×	×	√	√	√	√	Linux e Windows	Verificação automática no início da manhã todos os dias
	Inicialização automática	Verificar as entradas de inicialização automática e coletar estatísticas sobre as alterações de entrada em tempo hábil.	×	×	√	√	√	√	Linux e Windows	Verificação em tempo real

Função	Item	Descrição	Edição básica	Edição profissional	Edição empresarial	Edição premium	Edição WTP	Edição de container	SO suportado	Frequência de verificação
	Aplicação Web	Verificar detalhes sobre o software usado para push e lançamento de conteúdo da Web, incluindo versões, caminhos, arquivos de configuração e processos vinculados de todos os softwares.	×	×	√	√	√	√	Linux e Windows (somente o Tomcat é suportado)	Uma vez por semana (05:00 da manhã todas as segundas-feiras)
	Serviços Web	Verificar detalhes sobre o software usado para acesso ao conteúdo da Web, incluindo versões, caminhos, arquivos de configuração e processos vinculados de todos os softwares.	×	×	√	√	√	√	Linux	Uma vez por semana (05:00 da manhã todas as segundas-feiras)
	Estrutura Web	Verificar estatísticas sobre estruturas usadas para apresentação de conteúdo da Web, incluindo suas versões, caminhos e processos vinculados.	×	×	√	√	√	√	Linux	Uma vez por semana (05:00 da manhã todas as segundas-feiras)

Função	Item	Descrição	Edição básica	Edição profissional	Edição empresarial	Edição premium	Edição WTP	Edição de container	SO suportado	Frequência de verificação
	Site	Verificar as estatísticas sobre diretórios da Web e sites que podem ser acessados a partir da Internet. Você pode visualizar os diretórios e permissões, caminhos de acesso, portas externas, e processos principais de sites.	×	×	√	√	√	√	Linux	Uma vez por semana (05:00 da manhã todas as segundas-feiras)
	Middleware	Verificar informações sobre servidores, versões, caminhos e processos vinculados ao middleware.	×	×	√	√	√	√	Linux e Windows	Uma vez por semana (05:00 da manhã todas as segundas-feiras)
	Banco de dados	Verificar detalhes sobre o software que fornece armazenamento de dados, incluindo versões, caminhos, arquivos de configuração e processos vinculados de todos os softwares.	×	×	√	√	√	√	Linux e Windows (apenas MySQL é suportado)	Uma vez por semana (05:00 da manhã todas as segundas-feiras)

Função	Item	Descrição	Edição básica	Edição profissional	Edição empresarial	Edição premium	Edição WTP	Edição de container	SO suportado	Frequência de verificação
	Módulo do kernel	Verificar informações sobre todos os arquivos de módulo do programa em execução nos kernels, incluindo servidores vinculados, números de versão, descrições de módulos, caminhos de arquivos de drivers, permissões de arquivos e hashes de arquivos.	×	×	√	√	√	√	Linux	Uma vez por semana (05:00 da manhã todas as segundas-feiras)

Função	Item	Descrição	Edição básica	Edição profissional	Edição empresarial	Edição premium	Edição WTP	Edição de container	SO suportado	Frequência de verificação
Gerenciamento de vulnerabilidades	Detecção de vulnerabilidades do Linux	Com base no banco de dados de vulnerabilidades, verifique e trate vulnerabilidades no software (como kernel, OpenSSL, vim, glibc) que você obteve de fontes oficiais do Linux e não compilou.	√	√	√	√	√	√	Linux	• Verificação automática no início da manhã todos os dias • Verificação manual

Função	Item	Descrição	Edição básica	Edição profissional	Edição empresarial	Edição premium	Edição WTP	Edição de container	SO suportado	Frequência de verificação
	Detecção de vulnerabilidades do Windows	Detectar vulnerabilidades no SO Windows com base nos lançamentos de patches oficiais de Microsoft.	√	√	√	√	√	√	Windows	• Verificação automática no início da manhã todos os dias • Verificação manual

Função	Item	Descrição	Edição básica	Edição profissional	Edição empresarial	Edição premium	Edição WTP	Edição de container	SO suportado	Frequência de verificação
	Detecção de vulnerabilidade de Web-CMS	Procurar vulnerabilidades de Web-CMS em diretórios e arquivos da Web.	√	√	√	√	√	√	Linux e Windows	● Verificação automática no início da manhã todos os dias ● Verificação manual

Função	Item	Descrição	Edição básica	Edição profissional	Edição empresarial	Edição premium	Edição WTP	Edição de contaiener	SO suportado	Frequência de verificação
	Detecção de vulnerabilidades de aplicações	Detectar vulnerabilidades em pacotes JAR, arquivos ELF e outros arquivos de software de código aberto, como Log4j e spring-core.	×	×	√	√	√	√	Linux e Windows	• Uma vez por semana (05:00 da manhã todas as segundas-feiras) • Verificação manual

Função	Item	Descrição	Edição básica	Edição profissional	Edição empresarial	Edição premium	Edição WTP	Edição de container	SO suportado	Frequência de verificação
Verificação de configurações não seguras	Verificação da política de senha	Verificar as políticas de complexidade de senha e modificar-as com base nas sugestões fornecidas pelo HSS para melhorar a segurança da senha.	√	√	√	√	√	√	Linux	• Verificação automática no início da manhã todos os dias • Verificação manual

Função	Item	Descrição	Edição básica	Edição profissional	Edição empresarial	Edição premium	Edição WTP	Edição de container	SO suportado	Frequência de verificação
	Verificação de senha fraca	Alterar as senhas fracas por outras mais fortes com base nos resultados e sugestões da verificação do HSS.	√	√	√	√	√	√	Linux	• Verificação automática no início da manhã todos os dias • Verificação manual

Função	Item	Descrição	Edição básica	Edição profissional	Edição empresarial	Edição premium	Edição WTP	Edição de container	SO suportado	Frequência de verificação
	Configuração insegura	Verificar as configurações inseguras de Tomcat, Nginx e logon SSH encontradas pelo HSS.	×	×	√	√	√	√	Linux e Windows	● Verificação automática no início da manhã todos os dias ● Verificação manual

Função	Item	Descrição	Edição básica	Edição profissional	Edição empresarial	Edição premium	Edição WTP	Edição de container	SO suportado	Frequência de verificação
Segurança de imagens de containers	Gerenciamento de vulnerabilidade de imagem de container	Detectar e gerenciar vulnerabilidades em imagens locais e repositórios de imagens privadas com base em um banco de dados de vulnerabilidades e tratar vulnerabilidades críticas em tempo hábil.	×	×	×	×	×	√	Linux	● Verificação automática no início da manhã todos os dias ● Verificação manual
	Detecção de arquivo de imagem malicioso	Verificar imagens em busca de arquivos maliciosos (como cavalos de Troia, worms, vírus e adware) e identificar riscos.	×	×	×	×	×	√	Linux	Verificação em tempo real

Função	Item	Descrição	Edição básica	Edição profissional	Edição empresarial	Edição premium	Edição WTP	Edição de contaiiner	SO suportado	Frequência de verificação
	Verificação da linha de base da imagem	Verificar se há configurações inseguras com base em 18 tipos de linhas de base de container.	×	×	×	×	×	√	Linux	Verificação em tempo real
Proteção da aplicação	Injeção de SQL	Detectar e se defender contra ataques de injeção de SQL e verificar se há vulnerabilidades relacionadas em aplicações Web.	×	×	×	√	√	√	Linux	Verificação em tempo real
	Injeção de comando do SO	Detectar e se defender contra ataques remotos de injeção de comandos do SO e verificar se há vulnerabilidades relacionadas em aplicações Web.	×	×	×	√	√	√	Linux	Verificação em tempo real
	XSS	Detectar e se defender contra ataques de injeção de XSS (cross-site scripting) armazenados.	×	×	×	√	√	√	Linux	Verificação em tempo real
	Vulnerabilidade de Log4jRCE	Detectar e defender contra a execução remota de código.	×	×	×	√	√	√	Linux	Verificação em tempo real

Função	Item	Descrição	Edição básica	Edição profissional	Edição empresarial	Edição premium	Edição WTP	Edição de container	SO suportado	Frequência de verificação
	Carregamento de web shell	Detectar e defender-se contra ataques que carregam arquivos perigosos, alteram nomes de arquivos ou alteram tipos de extensão de nomes de arquivos; e verificar vulnerabilidades relacionadas em aplicações Web.	×	×	×	√	√	√	Linux	Verificação em tempo real
	Ataque XXE	Detectar e defender-se contra ataques de Injeção de entidade externa XML (XXE) e verificar aplicações Web em busca de vulnerabilidades relacionadas.	×	×	×	√	√	√	Linux	Verificação em tempo real
	Entrada de desserialização	Detectar ataques de desserialização que exploram classes inseguras.	×	×	×	√	√	√	Linux	Verificação em tempo real
	Passagem de diretório de arquivos	Verificar se diretórios ou arquivos sensíveis são acessados.	×	×	×	√	√	√	Linux	Verificação em tempo real

Função	Item	Descrição	Edição básica	Edição profissional	Edição empresarial	Edição premium	Edição WTP	Edição de container	SO suportado	Frequência de verificação
	Struts2 OGNL	Detectar a execução do código OGNL.	×	×	×	√	√	√	Linux	Verificação em tempo real
	Execução de comandos usando JSP	Detectar execução de comandos usando JSP.	×	×	×	√	√	√	Linux	Verificações em tempo real
	Exclusão de arquivos usando JSP	Detectar exclusão de arquivo usando JSP.	×	×	×	√	√	√	Linux	Verificação em tempo real
	Exceção de conexão de banco de dados	Detectar exceções de autenticação e comunicação lançadas por conexões de banco de dados.	×	×	×	√	√	√	Linux	Verificação em tempo real
	Vulnerabilidade do dia 0	Verificar se o hash de pilha de um comando está na lista branca da aplicação Web.	×	×	×	√	√	√	Linux	Verificação em tempo real

Função	Item	Descrição	Edição básica	Edição profissional	Edição empresarial	Edição premium	Edição WTP	Edição de container	SO suportado	Frequência de verificação
	Exceção de permissão SecurityManager	Detectar exceções lançadas pelo SecurityManager.	×	×	×	√	√	√	Linux	Verificação em tempo real
Prevenção de adulteração na página da Web	WTP estática	Proteger os arquivos de página da Web estáticos nos servidores do site de serem adulterados.	×	×	×	×	√	×	Linux e Windows	Verificação em tempo real
	WTP dinâmica	Fornecer proteção dinâmica contra adulteração na Web para o Tomcat. Proteger as páginas da Web dinâmicas em bancos de dados de sites de serem adulteradas.	×	×	×	×	√	×	Linux	Verificação em tempo real

Função	Item	Descrição	Edição básica	Edição profissional	Edição empresarial	Edição premium	Edição WTP	Edição de contentor	SO suportado	Frequência de verificação
Prevenção contra ransomware	Prevenção contra ransomware	Ajudar a identificar e detectar ataques de ransomware conhecidos e restaurar serviços usando backups.	×	×	×	√	√	√	Linux e Windows	Verificações em tempo real
Monitoramento da integridade de arquivos	Integridade do arquivo	Verificar os arquivos no SO Linux, aplicações e outros componentes para detectar adulteração.	×	×	×	√	√	√	Linux	Verificação em tempo real

Função	Item	Descrição	Edição básica	Edição profissional	Edição empresarial	Edição premium	Edição WTP	Edição de container	SO suportado	Frequência de verificação
Firewall de container	Firewall de container	Controlar e interceptar o tráfego de rede dentro e fora de um cluster de containers para evitar acesso e ataques maliciosos.	×	×	×	×	×	√	Linux	Verificação em tempo real
Controle de processo de aplicação	Controle de processo de aplicação	Aprender as características dos processos de aplicações em servidores e gerenciar sua execução. Processos suspeitos e confiáveis podem ser executados, e alarmes são gerados para processos maliciosos.	×	×	×	√	√	√	Linux e Windows	Verificação em tempo real
Proteção de cluster de containers	Proteção de cluster de containers	Verificar se há problemas de linha de base de não conformidade, vulnerabilidades e arquivos maliciosos quando uma imagem de container é iniciada e relatar alarmes ou bloquear a inicialização do container que não tenha sido não autorizada ou possa incorrer em altos riscos.	×	×	×	×	×	√	Linux	Verificação em tempo real

Função	Item	Descrição	Edição básica	Edição profissional	Edição empresarial	Edição premium	Edição WTP	Edição de container	SO suportado	Frequência de verificação
Detecção de intrusão	Malware não classificado	Verificar e tratar os programas maliciosos detectados em um só lugar, incluindo web shells, cavalos de Troia, software de mineração, worms e vírus.	×	√	√	√	√	√	Linux e Windows	Verificação em tempo real
	Vírus	Verificar os servidores em tempo real e relatar alarmes sobre vírus detectados nos servidores.	×	√	√	√	√	√	Linux e Windows	Verificação em tempo real
	Worm	Detectar e eliminar worms em servidores e relatar alarmes.	×	√	√	√	√	√	Linux e Windows	Verificação em tempo real
	Cavalo de Troia	Detectar programas que estão ocultos em programas normais e têm funções especiais, como danificar e excluir arquivos, enviar senhas e gravar teclados. Se um programa for detectado, um alarme será relatado imediatamente.	×	√	√	√	√	√	Linux e Windows	Verificação em tempo real

Função	Item	Descrição	Edição básica	Edição profissional	Edição empresarial	Edição premium	Edição WTP	Edição de contaiener	SO suportado	Frequência de verificação
	Botnet	Detectar se existem programas zumbis que foram espalhados nos servidores e relatar alarmes imediatamente após detectá-los.	×	√	√	√	√	√	Linux e Windows	Verificação em tempo real
	Web shell	Detectar ataques de web shell no sistema do servidor em tempo real e relatar alarmes imediatamente após detectá-los.	×	√	√	√	√	√	Linux e Windows	Verificação em tempo real
	Rootkit	Detectar ativos do servidor e relatar alarmes para módulos, arquivos e pastas do kernel suspeitos.	×	√	√	√	√	√	Linux	Verificação em tempo real
	Ransomware	Verificar ransomware incorporado em mídia, como páginas da Web, software, e-mails e mídia de armazenamento. O ransomware é usado para criptografar e controlar seus ativos de dados, como documentos, e-mails, bancos de dados, código-fonte, imagens e arquivos compactados, para alavancar a extorsão da vítima.	×	×	×	√	√	√	Linux e Windows	Verificação em tempo real

Função	Item	Descrição	Edição básica	Edição profissional	Edição empresarial	Edição premium	Edição WTP	Edição de container	SO suportado	Frequência de verificação
	Ferramenta de hacker	Verificar se existe alguma ferramenta não padrão usada para controlar o servidor e informar os alarmes imediatamente após detectá-los.	×	×	√	√	√	√	Linux e Windows	Verificação em tempo real
	Web shell	Você pode verificar se os arquivos (frequentemente arquivos PHP e JSP) em seus diretórios da Web são web shells. ● As informações do web shell incluem o caminho do arquivo do cavalo de Troia, o status, o horário da primeira descoberta e o horário da última descoberta. Você pode optar por ignorar o aviso em arquivos confiáveis. ● Você pode usar a função de detecção manual para fazer a verificação de web shells em servidores.	×	√	√	√	√	√	Linux e Windows	Verificação em tempo real

Função	Item	Descrição	Edição básica	Edição profissional	Edição empresarial	Edição premium	Edição WTP	Edição de contentainer	SO suportado	Frequência de verificação
	Mineração	Detectar se o software de mineração existe nos servidores em tempo real e relatar alarmes para o software detectado.	×	√	√	√	√	√	Linux e Windows	Verificação em tempo real
	Execução remota de código	Verificar se o servidor é chamado remotamente em tempo real e relatar um alarme imediatamente assim que a execução remota de código for detectada.	×	×	√	√	√	√	Linux e Windows	Verificação em tempo real
	Exploração da vulnerabilidade do Redis	Detectar as modificações feitas pelo processo do Redis nos principais diretórios em tempo real e relatar alarmes.	×	√	√	√	√	√	Linux	Verificação em tempo real
	Exploração da vulnerabilidade de Hadoop	Detectar as modificações feitas pelo processo de Hadoop nos principais diretórios em tempo real e relatar alarmes.	×	√	√	√	√	√	Linux	Verificação em tempo real

Função	Item	Descrição	Edição básica	Edição profissional	Edição empresarial	Edição premium	Edição WTP	Edição de container	SO suportado	Frequência de verificação
	Exploração da vulnerabilidade de MySQL	Detectar as modificações feitas pelo processo de MySQL nos principais diretórios em tempo real e relatar alarmes.	×	√	√	√	√	√	Linux	Verificação em tempo real
	Shell reverso	Monitorar os comportamentos do processo do usuário em tempo real para detectar e bloquear shells reversos causados por conexões inválidas. Os shells reversos podem ser detectados para protocolos, incluindo TCP, UDP e ICMP. **NOTA** Para ativar o bloqueio automático de shell reverso, execute as seguintes operações: 1. **Ative o bloqueio automático de shell reverso** ou **detecção e bloqueio automáticos de HIPS.** 2. **Isole e elimine programas maliciosos**.	×	√	√	√	√	√	Linux	Verificação em tempo real

Função	Item	Descrição	Edição básica	Edição profissional	Edição empresarial	Edição premium	Edição WTP	Edição de contaiener	SO suportado	Frequência de verificação
	Escalonamento de privilégio de arquivo	Verificar os escalonamentos de privilégios de arquivos em seu sistema.	×	√	√	√	√	√	Linux	Verificação em tempo real
	Escalonamento de privilégio do processo	As seguintes operações de escalonamento de privilégios de processo podem ser detectadas: ● Escalonamento de privilégio de raiz explorando vulnerabilidades do programa SUID ● Escalonamento de privilégios de raiz explorando vulnerabilidades do kernel	×	√	√	√	√	√	Linux	Verificação em tempo real
	Alteração no arquivo crítico	Receber alarmes quando arquivos críticos do sistema forem modificados.	×	√	√	√	√	√	Linux	Verificação em tempo real

Função	Item	Descrição	Edição básica	Edição profissional	Edição empresarial	Edição premium	Edição WTP	Edição de container	SO suportado	Frequência de verificação
	Alteração de arquivo/diretório	Monitorar arquivos e diretórios do sistema em tempo real e gerar alarmes se esses arquivos forem criados, excluídos, movidos ou se seus atributos ou conteúdo forem modificados.	×	√	√	√	√	√	Linux e Windows	Verificação em tempo real
	Comportamento anormal do processo	Verificar os processos em servidores, incluindo seus IDs, linhas de comando, caminhos de processo e comportamento. Enviar alarmes sobre operações de processo não autorizadas e intrusões. O seguinte comportamento anormal do processo pode ser detectado: ● Uso anormal da CPU ● Processos de acesso a endereços IP maliciosos ● Aumento anormal nas conexões de processos simultâneos	×	×	√	√	√	√	Linux e Windows	Verificação em tempo real

Função	Item	Descrição	Edição básica	Edição profissional	Edição empresarial	Edição premium	Edição WTP	Edição de container	SO suportado	Frequência de verificação
	Execução de comandos de alto risco	Receber alarmes em tempo real em comandos de alto risco.	×	√	√	√	√	√	Linux e Windows	Verificação em tempo real
	Shell anormal	Detectar ações em shells anormais, incluindo mover, copiar e excluir arquivos de shell e modificar as permissões de acesso e links físicos dos arquivos.	×	√	√	√	√	√	Linux	Verificação em tempo real
	Tarefa suspeita de crontab	Verificar e listar serviços iniciados automaticamente, tarefas agendadas, bibliotecas dinâmicas pré-carregadas, chaves de registro de execução e pastas de inicialização. Você pode ser notificado imediatamente quando itens anormais de inicialização automática forem detectados e localizar rapidamente os cavalos de Troia.	×	×	×	√	√	√	Linux e Windows	Verificação em tempo real

Função	Item	Descrição	Edição básica	Edição profissional	Edição empresarial	Edição premium	Edição WTP	Edição de contaiiner	SO suportado	Frequência de verificação
	Desativação da proteção do sistema	Detectar os preparativos para a criptografia de ransomware: desativar a função de proteção em tempo real do Windows Defender através do registro. Uma vez que a função é desativada, um alarme é relatado imediatamente.	×	×	√	√	√	×	Windows	Verificação em tempo real
	Exclusão de backup	Detectar os preparativos para a criptografia de ransomware: excluir arquivos de backup ou arquivos na pasta **Backup**. Uma vez que a exclusão de backup é detectada, um alarme é relatado imediatamente.	×	×	√	√	√	√	Windows	Verificação em tempo real
	Operação de registro suspeita	Detectar operações como desativar o firewall do sistema através do registro e usar o ransomware **Stop** para modificar o registro e gravar cadeias específicas no registro. Um alarme é relatado imediatamente quando essas operações são detectadas.	×	×	√	√	√	√	Windows	Verificação em tempo real

Função	Item	Descrição	Edição básica	Edição profissional	Edição empresarial	Edição premium	Edição WTP	Edição de contaiener	SO suportado	Frequência de verificação
	Exclusão do registo do sistema	Um alarme é gerado quando um comando ou ferramenta é usada para limpar logs do sistema.	×	×	√	√	√	×	Windows	Verificação em tempo real
	Execução de comandos suspeitos	● Verificar se uma tarefa agendada ou uma tarefa de inicialização automatizada é criada ou excluída executando comandos ou ferramentas. ● Detectar execução de comandos remotos suspeitos.	×	×	√	√	√	√	Linux e Windows	Verificação em tempo real
	Execução de processo suspeito	Detectar e relatar alarmes em processos de aplicações não autenticados ou não autorizados.	×	×	√	√	√	×	Linux e Windows	Verificação em tempo real
	Acesso ao arquivo de processo suspeito	Detectar e relatar alarmes nos processos de aplicações não autenticados ou não autorizados que acessam diretórios específicos.	×	×	√	√	√	×	Linux e Windows	Verificação em tempo real

Função	Item	Descrição	Edição básica	Edição profissional	Edição empresarial	Edição premium	Edição WTP	Edição de container	SO suportado	Frequência de verificação
	Defesa de ataque de força bruta	Verificar se há tentativas de ataque de força bruta e ataques de força bruta bem-sucedidos. ● Suas contas estão protegidas contra ataques de força bruta. O HSS bloqueará os hosts atacantes ao detectar esses ataques. ● O HSS relata um alarme se uma conta for quebrada e usada para fazer logon em um host com sucesso.	√	√	√	√	√	√	Linux e Windows	Verificação em tempo real
	Logon anormal	Verificar e lidar com logons remotos. Se a localização de logon de um usuário não for qualquer localização de logon comum que você definiu, um alarme será acionado.	√	√	√	√	√	√	Linux e Windows	Verificação em tempo real
	Conta inválida	Verificar contas em servidores e listar contas suspeitas em tempo hábil.	×	√	√	√	√	√	Linux e Windows	Verificação em tempo real

Função	Item	Descrição	Edição básica	Edição profissional	Edição empresarial	Edição premium	Edição WTP	Edição de contaiNer	SO suportado	Frequência de verificação
	Conta de usuário adicionada	Detectar os comandos usados para criar contas ocultas. As contas ocultas não podem ser encontradas na interface de interação com o usuário nem ser consultadas por comandos.	×	×	√	√	√	√	Windows	Verificação em tempo real
	Roubo de senha	Detectar a obtenção anormal de valor de hash de contas do sistema e senhas em servidores e relatar alarmes.	×	×	√	√	√	√	Linux e Windows	Verificação em tempo real
	Conexão de saída anormal	Relatar alarmes sobre endereços IP suspeitos que iniciam conexões de saída.	×	√	√	√	√	√	Linux	Verificação em tempo real
	Encaminhamento de porta	Relatar alarmes no encaminhamento de porta usando ferramentas suspeitas.	×	√	√	√	√	√	Linux	Verificação em tempo real
	Solicitação de download suspeita	Um alarme é gerado quando uma solicitação HTTP suspeita que usa ferramentas do sistema para baixar programas é detectada.	×	×	√	√	√	×	Windows	Verificação em tempo real

Função	Item	Descrição	Edição básica	Edição profissional	Edição empresarial	Edição premium	Edição WTP	Edição de contai ner	SO suportado	Frequência de verificação
	Solicitação HTTP suspeita	Um alarme é gerado quando uma solicitação HTTP suspeita que usa uma ferramenta ou processo do sistema para executar um script de hospedagem remota é detectada.	×	×	√	√	√	×	Windows	Verificação em tempo real
	Verificação da porta	Detectar verificação ou farejamento em portas especificadas e relatar alarmes.	×	×	×	√	√	√	Linux	Verificação em tempo real
	Verificação do host	Detectar as atividades de verificação de rede com base nas regras do servidor (incluindo ICMP, ARP e nbtscan) e informar alarmes.	×	×	×	√	√	√	Linux	Verificação em tempo real

Função	Item	Descrição	Edição básica	Edição profissional	Edição empresarial	Edição premium	Edição WTP	Edição de container	SO suportado	Frequência de verificação
Detecção de intrusão de container (tempo de execução do container: Docker e Containerd)	Malware não classificado	Verificar e tratar programas maliciosos em um container, incluindo web shells, cavalos de Troia, software de mineração, worms e vírus.	×	×	×	×	×	√	Linux	Verificação em tempo real
	Ransomware	Verificar e gerenciar alarmes sobre ransomware em containers.	×	×	×	×	×	√	Linux	Verificação em tempo real
	Web shell	Verificar se os arquivos (frequentemente arquivos PHP e JSP) nos diretórios da Web em containers são web shells.	×	×	×	×	×	√	Linux	Verificação em tempo real
	Escape de vulnerabilidade	Um alarme de escape é relatado se for detectado um comportamento de processo de container que corresponda ao comportamento de vulnerabilidades conhecidas.	×	×	×	×	×	√	Linux	Verificações em tempo real

Função	Item	Descrição	Edição básica	Edição profissional	Edição empresarial	Edição premium	Edição WTP	Edição de container	SO suportado	Frequência de verificação
	Escape de arquivo	Um alarme é relatado se um processo de container é encontrado acessando um diretório de arquivo de chave (por exemplo, **/etc/shadow** ou **/etc/crontab**). Diretórios que atendem às regras de mapeamento de diretório de container também podem acionar esses alarmes.	×	×	×	×	×	√	Linux	Verificação em tempo real
	Shell reverso	Monitorar o comportamento do processo do usuário em tempo real para detectar shells reversos causados por conexões inválidas. Os shells reversos podem ser detectados para protocolos, incluindo TCP, UDP e ICMP.	×	×	×	×	×	√	Linux	Verificação em tempo real

Função	Item	Descrição	Edição básica	Edição profissional	Edição empresarial	Edição premium	Edição WTP	Edição de container	SO suportado	Frequência de verificação
	Escalonamento de privilégio do processo	As seguintes operações de escalonamento de privilégios de processo podem ser detectadas: ● Escalonamento de privilégio de raiz explorando vulnerabilidades do programa SUID ● Escalonamento de privilégios de raiz explorando vulnerabilidades do kernel	×	×	×	×	×	√	Linux	Verificação em tempo real
	Execução de comandos de alto risco	Verificar comandos executados em containers e gerar alarmes se comandos de alto risco forem detectados.	×	×	×	×	×	√	Linux	Verificação em tempo real

Função	Item	Descrição	Edição básica	Edição profissional	Edição empresarial	Edição premium	Edição WTP	Edição de container	SO suportado	Frequência de verificação
	Processo de container anormal	● Programa de container malicioso Monitorar o comportamento do processo do container e processar as impressões digitais do arquivo. Um alarme é reportado se detectar um processo cujas características de comportamento correspondem às de um programa malicioso predefinido. ● Processo anormal Um alarme é relatado se um processo que não está na lista branca estiver sendo executado no container.	×	×	×	×	×	√	Linux	Verificação em tempo real

Função	Item	Descrição	Edição básica	Edição profissional	Edição empresarial	Edição premium	Edição WTP	Edição de container	SO suportado	Frequência de verificação
	Inicialização anormal do container	O serviço monitora inicialização de container e relata um alarme se detectar que um container com muitas permissões foi iniciado. Os itens de verificação de container incluem: ● Inicialização de container privilegiado (**privileged:true**) ● Muitos recursos de container (**capability:[xxx]**) ● Seccomp não ativado (**seccomp=unconfined**) ● Escalonamento de privilégios de container(**no-new-privileges:false**) ● Mapeamento de diretório de alto risco (**mounts:[...]**)	×	×	×	×	×	√	Linux	Verificação em tempo real
	Chamada de sistema de alto risco	Você pode executar tarefas em kernels por chamadas de sistema do Linux. A edição de container relata um alarme se detectar uma chamada de alto risco.	×	×	×	×	×	√	Linux	Verificação em tempo real

Função	Item	Descrição	Edição básica	Edição profissional	Edição empresarial	Edição premium	Edição WTP	Edição de container	SO suportado	Frequência de verificação
	Bloqueio da imagem do container	Se um container contiver imagens inseguras especificadas em **Comportamentos suspeitos de imagem**, um alarme será gerado e as imagens inseguras serão bloqueadas antes que um container seja iniciado no Docker. **NOTA** Você precisa **instalar o plug-in do Docker**.	×	×	×	×	×	√	Linux	Verificação em tempo real
	Acesso a arquivos confidenciais	O serviço monitora os arquivos de imagem de container vinculados às políticas de proteção de arquivos e relatar um alarme se os arquivos forem modificados.	×	×	×	×	×	√	Linux	Verificação em tempo real

Função	Item	Descrição	Edição básica	Edição profissional	Edição empresarial	Edição premium	Edição WTP	Edição de contaiiner	SO suportado	Frequência de verificação
	Ataque de força bruta	Detectar e relatar alarmes para comportamentos de ataque de força bruta, como tentativas de ataque de força bruta e ataques de força bruta bem-sucedidos, em containers. Detectar ataques de força bruta SSH, Web e Enumdb em containers. **NOTA** Atualmente, os ataques de força bruta podem ser detectados apenas no tempo de execução do Docker.	×	×	×	×	×	√	Linux	Verificação em tempo real
	Conta de usuário do sistema inválida	Detectar contas suspeitas e relatar alarmes.	×	×	×	×	×	√	Linux	Verificação em tempo real
	Comportamento anormal do pod	Detectar operações anormais, como a criação de pods privilegiados, pods estáticos e pods sensíveis em um cluster e operações anormais executadas em pods existentes e relatar alarmes.	×	×	×	×	×	√	Linux	Verificação em tempo real

Função	Item	Descrição	Edição básica	Edição profissional	Edição empresarial	Edição premium	Edição WTP	Edição de contaiiner	SO suportado	Frequência de verificação
	Enumeração de informações do usuário	Detectar as operações de enumerar as permissões e a lista de operações executáveis dos usuários do cluster e relatar alarmes.	×	×	×	×	×	√	Linux	Verificação em tempo real
	Vinculação de função de cluster	Detectar operações como vinculação ou criação de uma função de cluster de alto privilégio ou conta de serviço e relatar alarmes.	×	×	×	×	×	√	Linux	Verificação em tempo real
	Exclusão de eventos do Kubernetes	Detectar a exclusão de eventos do Kubernetes e relatar alarmes.	×	×	×	×	×	√	Linux	Verificação em tempo real

Função	Item	Descrição	Edição básica	Edição profissional	Edição empresarial	Edição premium	Edição WTP	Edição de container	SO suportado	Frequência de verificação
Gerenciamento de listas brancas	Lista branca do alarme	Você pode adicionar um alarme à lista branca ao manuseá-lo.	×	√	√	√	√	√	Linux e Windows	Verificação em tempo real
	Lista branca de logon	Adicionar endereços IP e nomes de usuário à lista branca de logon, conforme necessário. O HSS não relatará alarmes sobre os comportamentos de acesso desses endereços IP e usuários.	×	√	√	√	√	√	Linux e Windows	Verificação em tempo real
	Lista branca do usuário do sistema	Os usuários (usuários não raiz) recém-adicionados ao grupo de usuários raiz em um servidor podem ser adicionados à lista branca de usuários do sistema. O HSS não relatará alarmes de conta arriscados para eles.	×	√	√	√	√	√	Linux e Windows	Verificação em tempo real

Função	Item	Descrição	Edição básica	Edição profissional	Edição empresarial	Edição premium	Edição WTP	Edição de container	SO suportado	Frequência de verificação
Gerenciamento de políticas	Consultar e editar configurações de regras	Você pode definir e emitir diferentes políticas de detecção para diferentes servidores ou grupos de servidores, implementando operações de segurança refinadas. ● Visualizar a lista de políticas. ● Criar um grupo de políticas com base em grupos de políticas padrão e existentes. ● Definir uma política. ● Editar ou excluir uma política. ● Modificar ou desativar políticas em um grupo. ● Aplicar políticas a servidores em lotes na página **Servers & Quota**.	×	√ (Somente o grupo de políticas profissionais padrão é suportado.)	√ (Somente o grupo de políticas empresariais padrão é suportado.)	√	√	√	Linux e Windows	Verificação em tempo real

Função	Item	Descrição	Edição básica	Edição profissional	Edição empresarial	Edição premium	Edição WTP	Edição de contaiener	SO suportado	Frequência de verificação
Histórico de manipulação	Histórico de manipulação	Verificar os registros históricos de vulnerabilidade e manipulação de alarmes, incluindo o tempo de manipulação e os manipuladores.	×	√	√	√	√	√	Linux e Windows	-
Relatório de segurança	Relatório de segurança do servidor	Verificar semanalmente ou mensalmente as tendências de segurança do servidor, os principais eventos de segurança e os riscos.	×	√	√	√	√	√	Linux e Windows	-
Configuração de segurança	Gerenciamento do agente	Você pode visualizar o status do agente de todos os servidores e atualizar, desinstalar e instalar agentes.	√	√	√	√	√	√	Linux e Windows	Verificação em tempo real

Função	Item	Descrição	Edição básica	Edição profissional	Edição empresarial	Edição premium	Edição WTP	Edição de container	SO suportado	Frequência de verificação
	Localização de logon comum	Para cada servidor, você pode configurar as localizações de onde os usuários costumam fazer logon. O serviço gerará alarmes em logons originados de localizações diferentes das localizações de logon comuns configuradas. Um servidor pode ser adicionado a várias localizações de logon.	√	√	√	√	√	√	Linux e Windows	Verificação em tempo real
	Endereço IP de logon comum	Para cada servidor, você pode configurar os endereços IP de onde os usuários geralmente fazem logon. O serviço gerará alarmes em logons originados de endereços IP diferentes dos endereços IP comuns configurados.	√	√	√	√	√	√	Linux e Windows	Verificação em tempo real

Função	Item	Descrição	Edição básica	Edição profissional	Edição empresarial	Edição premium	Edição WTP	Edição de contaiener	SO suportado	Frequência de verificação
	Configurar uma lista branca de endereços IP de logon SSH	A lista branca de logon SSH controla o acesso SSH aos servidores para evitar quebra de conta. Depois de configurar a lista branca, os logons SSH serão permitidos apenas a partir de endereços IP na lista branca.	√	√	√	√	√	√	Linux	Verificação em tempo real
	Isolamento e remoção de programas maliciosos	O HSS isola e elimina automaticamente os programas maliciosos identificados, como web shells, cavalos de Troia e worms, eliminando riscos de segurança.	×	√	√	√	√	√	Linux e Windows	Verificação em tempo real
	2FA	Evitar ataques de força bruta usando senha e autenticação de SMS/e-mail.	Pagamento por uso: × Anual/mensal: √	√	√	√	√	√	Linux e Windows	-

Função	Item	Descrição	Edição básica	Edição profissional	Edição empresarial	Edição premium	Edição WTP	Edição de container	SO suportado	Frequência de verificação
	Configuração de alarme	Depois que a notificação de alarme estiver ativada, você poderá receber notificações de alarme enviadas pelo HSS para aprender sobre os riscos de segurança enfrentados por seus servidores, containers e páginas da Web.	√	√	√	√	√	√	Linux e Windows	-

Função	Item	Descrição	Edição básica	Edição profissional	Edição empresarial	Edição premium	Edição WTP	Edição de container	SO suportado	Frequência de verificação
Autoproteção do HSS	Autoproteção do HSS	Proteger arquivos, processos e softwares do HSS contra programas maliciosos, que podem desinstalar agentes do HSS, adulterar arquivos do HSS ou interromper processos do HSS. ● A autoproteção depende da detecção de antivírus, detecção de HIPS e proteção contra ransomware. Ela só entra em vigor quando mais de uma das três funções estiver ativada. ● A ativação da política de autoproteção tem os seguintes impactos: – O agente do HSS não pode ser desinstalado no painel de controle de um servidor, mas pode ser desinstalado no console do HSS.	×	×	×	√	√	×	Windows	-

Função	Item	Descrição	Edição básica	Edição profissional	Edição empresarial	Edição premium	Edição WTP	Edição de container	SO suportado	Frequência de verificação
		– Os processos do HSS não podem ser encerrados. – No caminho de instalação do agente **C:\Program Files \HostGuard**, você só pode acessar os diretórios de **log** e **data** (e o diretório de **upgrade**, se o seu agente tiver sido atualizado).								

4 Cenários

HSS

- Conformidade com o esquema de proteção multinível (MLPS) de DJCP

  A função de detecção de intrusão do HSS protege contas e sistemas em servidores em nuvem, ajudando as empresas a atender aos padrões de conformidade.

  Para solicitar a certificação MLPS de DJCP, adquira a edição empresarial ou uma edição superior (edição premium ou edição de Proteção contra adulteração na Web).

- Gerenciamento centralizado de segurança

  Com o HSS, você pode gerenciar as configurações e eventos de segurança de todos os seus servidores em nuvem no console, reduzindo riscos e custos de gerenciamento.

- Avaliação dos riscos de segurança

  Você pode verificar e eliminar todos os riscos (como contas arriscadas, portas abertas, vulnerabilidades de software e senhas fracas) em seus servidores.

- Proteção de contas

  Aproveitar os recursos abrangentes de segurança de contas, incluindo prevenção, anti-ataque e verificação pós-ataque. Você pode usar a 2FA para bloquear ataques de força bruta em contas, aumentando a segurança de seus servidores em nuvem.

- Segurança proativa

  Contar e verificar os ativos do seu servidor, verificar e corrigir vulnerabilidades e configurações inseguras e proteger proativamente sua rede, aplicações e arquivos contra ataques.

- Detecção de intrusão

  Verificar todos os vetores de ataques possíveis para detectar e combater ameaças persistentes avançadas (APTs) e outras ameaças em tempo real, protegendo seu sistema do impacto.

CGS

- Segurança de imagens de containers

  As vulnerabilidades provavelmente serão introduzidas no seu sistema por meio das imagens baixadas do Docker Hub ou por meio de estruturas de código aberto.

  Você pode usar o CGS para verificar imagens em busca de riscos, incluindo vulnerabilidades de imagem, contas inseguras e arquivos maliciosos. Receba lembretes e sugestões e elimine os riscos de acordo.

- Segurança de tempo de execução de containers

  Desenvolver uma lista branca de comportamentos de containers para garantir que os containers sejam executados com as permissões mínimas necessárias, protegendo os containers contra possíveis ameaças.

- Conformidade com MLPS de DJCP

  Evitar invasões e códigos maliciosos, garantindo que a segurança do seu container e do sistema atenda aos requisitos de conformidade.

5 Restrições

Tipos de servidores suportados

- ECS
- BMS
- Huawei Cloud Workspace
- Servidor de nuvem de terceiros
- Servidor local

NOTA

Atualmente, apenas algumas regiões suportam o acesso a servidores não da Huawei Cloud. Para obter detalhes sobre as regiões, consulte **Onde o HSS está disponível?**

SOs suportados

O HSS usa o agente para monitorar riscos de segurança e se defender contra invasões externas. Para proteger um servidor com HSS, certifique-se de que o agente esteja ativo e em execução no servidor. Para obter mais informações, consulte **Tabela 5-1**.

AVISO

- O agente é provavelmente incompatível com as versões de Linux ou Windows que atingiram o fim da vida útil. Para obter uma melhor experiência de serviço HSS, é aconselhável instalar ou atualizar para uma versão do SO suportada pelo agente.
- Se um software de segurança de terceiros, como o McAfee tiver sido instalado no servidor, interrompa a função de proteção do software antes de instalar um agente do HSS. Depois de instalar o agente, você pode reativar a função de proteção no software.
- O CentOS 6.x não é mais atualizado ou mantido no site oficial do Linux, e o HSS não suporta mais o CentOS 6.x ou anterior.

Tabela 5-1 SOs suportados

Tipo de SO	Arquitetura do sistema	Versão do SO suportada	Suporte para verificação de vulnerabilidades
Windows	X86	Windows 10 (64-bit) **NOTA** Somente o Huawei Cloud Workspace pode usar este sistema operacional.	×
		Windows 11 (64-bit) **NOTA** Somente o Huawei Cloud Workspace pode usar este sistema operacional.	×
		Windows Server 2012 R2 Standard 64-bit English (40 GB)	√
		Windows Server 2012 R2 Standard 64-bit Chinese (40 GB)	√
		Windows Server 2012 R2 Datacenter 64-bit English (40 GB)	√
		Windows Server 2012 R2 Datacenter 64-bit Chinese (40 GB)	√
		Windows Server 2016 Standard 64-bit English (40 GB)	√
		Windows Server 2016 Standard 64-bit Chinese (40 GB)	√
		Windows Server 2016 Datacenter 64-bit English (40 GB)	√
		Windows Server 2016 Datacenter 64-bit Chinese (40 GB)	√
		Windows Server 2019 Datacenter 64-bit English (40 GB)	√
		Windows Server 2019 Datacenter 64-bit Chinese (40 GB)	√
Linux	X86	CentOS 7.4 (64-bit)	√
		CentOS 7.5 (64-bit)	√
		CentOS 7.6 (64-bit)	√
		CentOS 7.7 (64-bit)	√
		CentOS 7.8 (64-bit)	√
		CentOS 7.9 (64-bit)	√

Tipo de SO	Arquitetura do sistema	Versão do SO suportada	Suporte para verificação de vulnerabilidades
		CentOS 8.0 (64-bit)	×
		CentOS 8.1 (64-bit)	×
		CentOS 8.2 (64-bit)	×
		CentOS 8 (64-bit)	×
		CentOS 9 (64-bit)	×
		Debian 9 (64-bit)	√
		Debian 10 (64-bit)	√
		Debian 11.0.0 (64-bit)	√
		Debian 11.1.0 (64-bit)	√
		EulerOS 2.2 (64-bit)	√
		EulerOS 2.3 (64-bit)	√
		EulerOS 2.5 (64-bit)	√
		EulerOS 2.7 (64-bit)	×
		EulerOS 2.9 (64-bit)	√
		Fedora 28 (64-bit)	×
		Ubuntu 16.04 (64-bit)	√
		Ubuntu 18.04 (64-bit)	√
		Ubuntu 20.03 (64-bit)	×
		Ubuntu 20.04 (64-bit)	√
		Ubuntu 22.04 (64-bit)	×
		Red Hat 7.4 (64-bit)	×
		Red Hat 7.6 (64-bit)	×
		Red Hat 8.0 (64-bit)	×
		Red Hat 8.7 (64-bit)	×
		OpenEuler 20.03 LTS (64-bit)	×
		OpenEuler 22.03 SP3 (64-bit)	×
		OpenEuler 22.03 (64-bit)	×
		AlmaLinux 9.0 (64-bit)	×

Tipo de SO	Arquitetura do sistema	Versão do SO suportada	Suporte para verificação de vulnerabilidades
		Rocky Linux 8.4 (64-bit)	×
		Rocky Linux 8.5 (64-bit)	×
		Rocky Linux 9.0 (64-bit)	×
		HCE 2.0 (64-bit)	×
		SUSE 12 SP5 (64-bit)	√
		SUSE 15 SP2 (64-bit)	√
		SUSE 15.5 (64-bit)	√
	ARM	CentOS 7.4 (64-bit)	√
		CentOS 7.5 (64-bit)	√
		CentOS 7.6 (64-bit)	√
		CentOS 7.7 (64-bit)	√
		CentOS 7.8 (64-bit)	√
		CentOS 7.9 (64-bit)	√
		CentOS 8.0 (64-bit)	×
		CentOS 8.1 (64-bit)	×
		CentOS 8.2 (64-bit)	×
		CentOS 9 (64-bit)	×
		EulerOS 2.8 (64-bit)	√
		EulerOS 2.9 (64-bit)	√
		Fedora 29 (64-bit)	×
		Ubuntu 18 (64-bit)	×
		Kylin V7 (64-bit)	×
		Kylin V10 (64-bit)	√
		HCE 2.0 (64-bit)	×
		UnionTech OS V20 (64-bit)	√ (Edições E e D do servidor UOS V20)

6 Mecanismo de proteção de dados pessoais

Para garantir que seus dados pessoais, como seu nome de usuário, senha e número de telefone celular, não serão violados por entidades ou pessoas não autorizadas ou não autenticadas, o HSS criptografa seus dados pessoais antes de armazená-los e controla o acesso aos dados.

Dados pessoais

Tabela 6-1 descreve os dados pessoais gerados ou recolhidos pelo HSS.

Tabela 6-1 Dados pessoais

Tipo	Método de coleta	Pode ser modificado	Obrigatório
E-mail	Se a 2FA estiver ativada, o HSS obterá periodicamente de SMN os endereços de e-mail que assinam os tópicos de notificação.	Não	Sim
Número de celular	Se a 2FA estiver ativada, o HSS obterá periodicamente de SMN os números de telefones celulares que assinam os tópicos de notificação.	Não	Sim
Localização do logon	Se o HSS estiver ativado, ele registrará as localizações de logon do usuário.	Não	Sim

Modo de armazenamento

O HSS usa algoritmos de criptografia para criptografar os dados confidenciais dos usuários e armazena dados criptografados.

- Os números de telefone celular são criptografados antes do armazenamento.
- As localizações de logon não são dados confidenciais e são armazenadas em texto simples.

Controle de acesso

Os dados pessoais do usuário são criptografados antes de serem armazenados no banco de dados do HSS. O mecanismo de lista branca é usado para controlar o acesso ao banco de dados.

7 Segurança

7.1 Responsabilidades compartilhadas

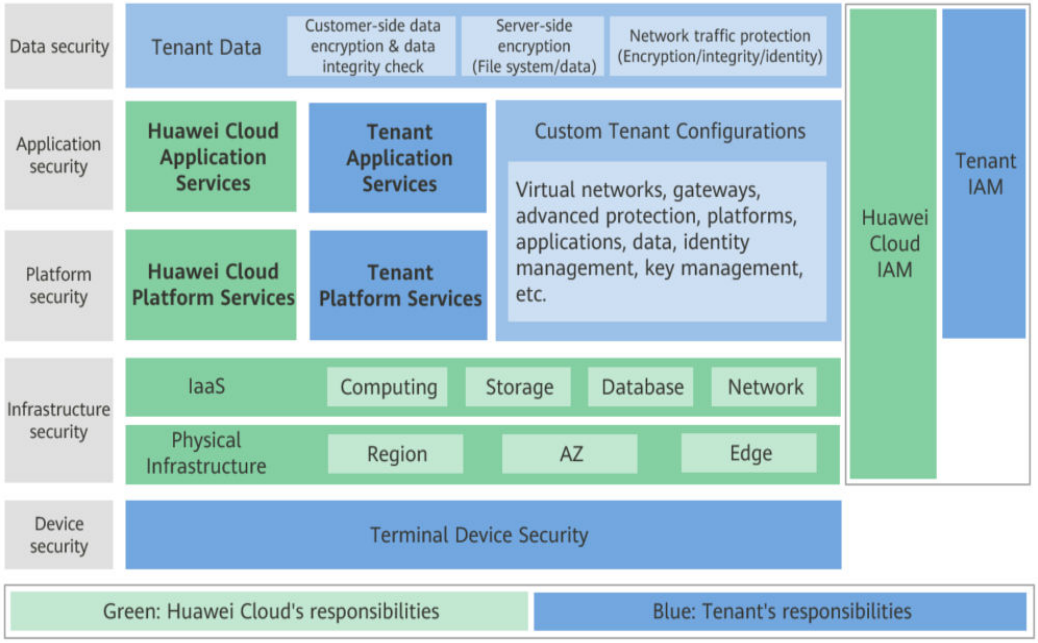
Huawei garante que seu compromisso com a segurança cibernética nunca será superado pela consideração de interesses comerciais. Para lidar com os desafios emergentes de segurança na nuvem e ameaças e ataques à segurança na nuvem, a Huawei Cloud constrói um sistema abrangente de garantia de segurança de serviços em nuvem para diferentes regiões e indústrias com base nas vantagens exclusivas de software e hardware da Huawei, leis, regulamentos, padrões da indústria e ecossistema de segurança.

Figura 7-1 ilustra as responsabilidades partilhadas pela Huawei Cloud e pelos usuários.

- **Huawei Cloud**: garante a segurança dos serviços de nuvem e fornece nuvens seguras. As responsabilidades de segurança da Huawei Cloud incluem garantir a segurança de nossos serviços de IaaS, PaaS e SaaS, bem como os ambientes físicos dos data centers da Huawei Cloud onde nossos serviços de IaaS, PaaS e SaaS operam. A Huawei Cloud é responsável não apenas pelas funções de segurança e pelo desempenho de nossa infraestrutura, serviços de nuvem e tecnologias, mas também pela segurança geral de O&M na nuvem e, no sentido mais amplo, pela certificação de segurança de nossa infraestrutura e serviços.
- **Locatário**: usa a nuvem com segurança. Os locatários da Huawei Cloud são responsáveis pelo gerenciamento seguro e eficaz das configurações personalizadas dos serviços em nuvem, incluindo IaaS, PaaS e SaaS. Isso inclui, mas não se limita a, redes virtuais, o SO de hosts e convidados de máquinas virtuais, firewalls virtuais, API Gateway, serviços avançados de segurança, todos os tipos de serviços em nuvem, dados de locatários, contas de identidade e gerenciamento de chaves.

O livro branco de segurança da Huawei Cloud elabora as ideias e medidas para a construção da segurança da Huawei Cloud, incluindo estratégias de segurança na nuvem, o modelo de responsabilidade compartilhada, conformidade e privacidade, organizações e pessoal de segurança, segurança de infraestrutura, serviço e segurança de locatários, segurança de engenharia, segurança de O&M e segurança do ecossistema.

Figura 7-1 Modelo de responsabilidade de segurança compartilhada da Huawei Cloud

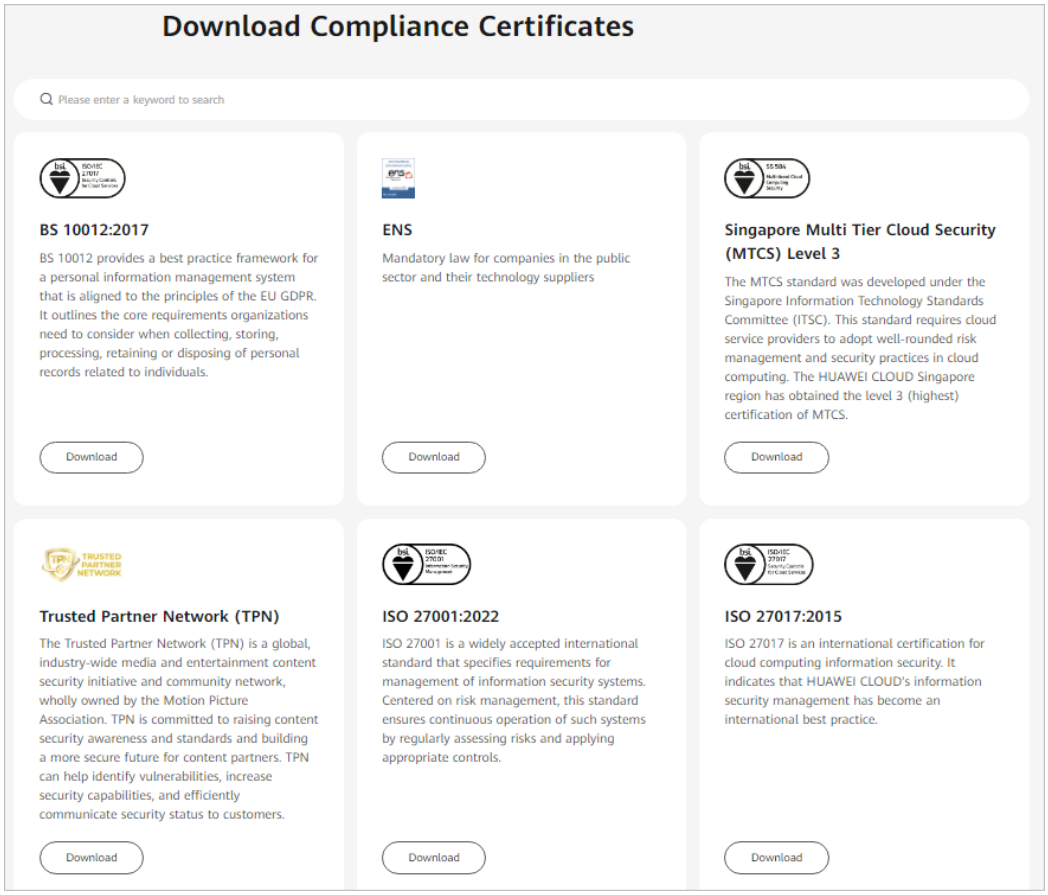


7.2 Certificados

Certificados de conformidade

Os serviços e plataformas da Huawei Cloud obtiveram várias certificações de segurança e de conformidade das organizações autorizadas, como a Organização Internacional de Normalização (ISO). Você pode **baixá-los** do console.

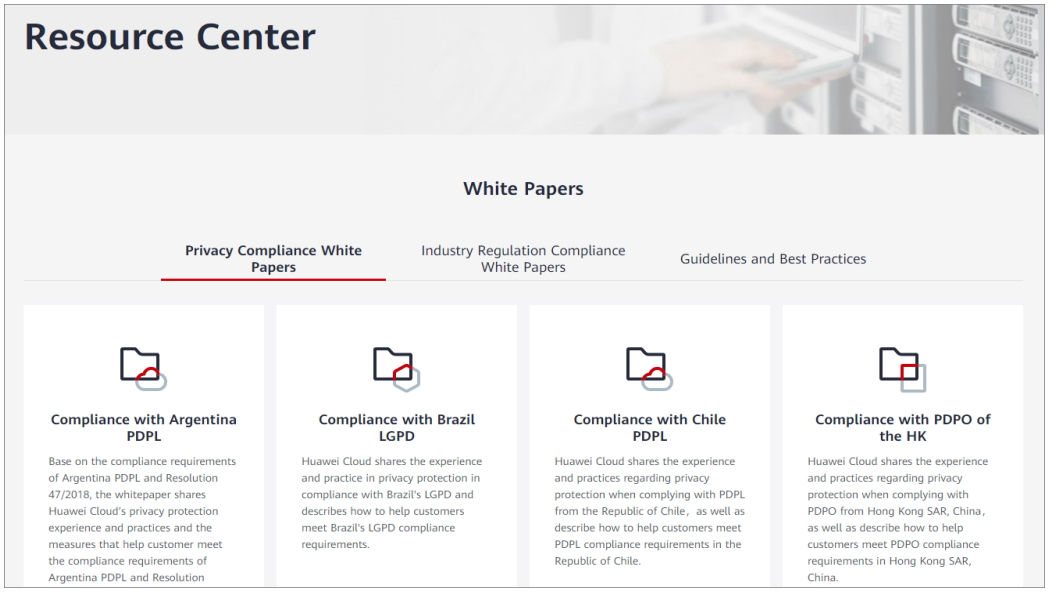
Figura 7-2 Download de certificados de conformidade



Central de recursos

A Huawei Cloud também fornece os seguintes recursos para ajudar os usuários a atender aos requisitos de conformidade. Para obter detalhes, consulte **Central de recursos**.

Figura 7-3 Central de recursos



7.3 Identificação e gerenciamento de ativos

O Host Security Service (HSS) coleta informações sobre ativos em seus servidores, como contas, processos, portas abertas, itens iniciados automaticamente, software, estruturas da Web, sites, middleware e módulos do kernel. Você pode aprender o status geral de seus ativos em um relance.

7.4 Autenticação de identidade e controle de acesso

Identity and Access Management (IAM) fornece gerenciamento de permissões refinado para recursos de HSS. Você pode:

- Criar usuários do IAM para funcionários com base na estrutura organizacional da sua empresa. Cada usuário do IAM tem suas próprias credenciais de segurança, fornecendo acesso aos recursos do HSS.
- Conceder apenas as permissões necessárias para que os usuários executem uma tarefa específica.
- Confiar em uma conta ou serviço de nuvem da Huawei Cloud para realizar O&M profissional e eficiente em seus recursos de HSS.

  Para obter detalhes sobre políticas de permissão do HSS, consulte **Criação de um usuário e concessão de permissões**.

7.5 Tecnologias de proteção de dados

O HSS toma medidas diferentes para manter os dados armazenados no HSS seguros e confiáveis.

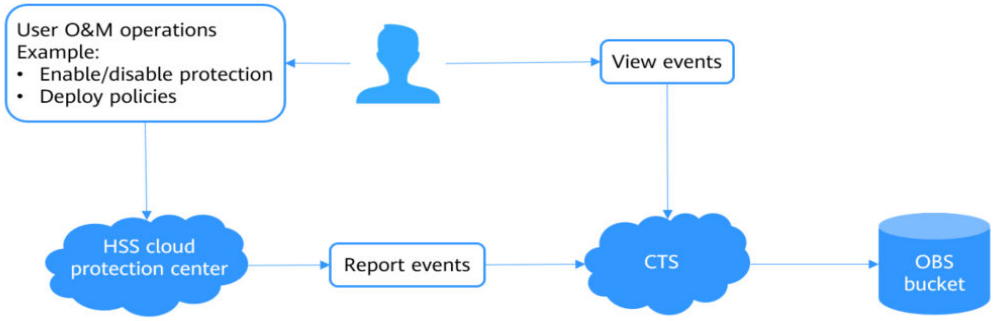
Medida	Descrição
Criptografia de transmissão (HTTPS)	Os dados são criptografados quando são transmitidos entre microsserviços para evitar vazamento ou adulteração durante a transmissão. Suas configurações são mantidas seguras quando transmitidas por HTTPS.
Redundância de dados	Dados como informações de ativos e eventos de alarme podem ser copiados e restaurados usando cópias.
Armazenamento de dados criptografados	O HSS criptografa dados sensíveis para evitar vazamentos.

Você também pode ativar a edição de Proteção contra adulteração na Web (WTP) para proteger os dados comerciais.

Para obter mais informações, consulte **Ativação da edição WTP**.

7.6 Auditoria e registro

O Cloud Trace Service (CTS) monitora as atividades do usuário e as alterações de recursos nos seus recursos de nuvem. Ele ajuda você a coletar, armazenar e consultar registros operacionais para análise de segurança, auditoria e conformidade e localização de falhas.



Para obter detalhes sobre como habilitar e configurar o CTS, consulte **Habilitação do CTS**.

Para obter detalhes sobre as operações de HSS que podem ser auditadas pelo CTS, consulte **Operações de HSS suportadas pelo CTS**.

7.7 Resiliência de serviço

O HSS usa uma arquitetura de confiabilidade de quatro níveis. Ele fornece recursos de inspeção, resistência e recuperação para ajudá-lo a recuperar manualmente ou automaticamente os serviços, aprimorando a durabilidade e a confiabilidade dos dados.

Tabela 7-1 Arquitetura de confiabilidade

Categoria	Capacidade	Descrição	Tipo
Inspeção	Situation Awareness (SA)	HSS interconecta-se com SA e avalia os riscos de ativos com base em alarmes, vulnerabilidades e resultados de verificação da linha de base.	Sistema
	Cloud Eye	Com o Cloud Eye, você pode entender o uso de recursos e o status do HSS, receber notificações de alarme em tempo hábil e reagir às alterações para manter seus serviços funcionando sem problemas.	Sistema
Resistência	Prevenção contra ataques	O agente fornece recursos de autoproteção, anti-remoção e anti-adulteração.	Segurança
	Backup de dados	Todos os dados-chave podem ser copiados. Mesmo que o banco de dados esteja completamente danificado, os serviços podem ser restaurados usando os dados de backup.	Sistema

Categoria	Capacidade	Descrição	Tipo
	Autoproteção de serviço	O HSS consiste em microsserviços, que são implementados, iniciados e interrompidos de forma independente. O agente controla estritamente seu uso de recursos. Se seu uso de recursos exceder o limite, o agente será isolado ou uma operação de bypass será executada para evitar afetar as cargas de trabalho do usuário. Se os recursos do sistema forem insuficientes, o desempenho do agente será degradado.	Sistema
Restauração	Restauração do sistema	Uma VM ou um serviço pode ser reconstruído manualmente ou automaticamente se estiver com defeito.	Sistema
	Proteção do processo	Se um processo for encerrado, o processo será iniciado automaticamente para facilitar a recuperação do serviço.	Sistema

7.8 Monitoramento de riscos

O Cloud Eye fornece monitoramento multidimensional para seus recursos na nuvem. Ele permite que você visualize o uso de recursos e o status de execução do serviço e responda a exceções em tempo hábil para garantir o bom funcionamento dos serviços.

O HSS usa o Cloud Eye para realizar o monitoramento de recursos e operações, ajudando a monitorar a segurança do servidor e a receber alarmes e notificações em tempo real. Você pode verificar o número de servidores desprotegidos, o número de servidores inseguros e o número de agentes que não estão instalados ou estão off-line em tempo real.

Para obter detalhes sobre métricas do HSS e como criar regras de alarme, consulte **Monitoramento**.

7.9 Retificação de falhas

Todos os componentes do HSS são implementados no modo primário/em espera ou modo de cluster para oferecer suporte a DR entre AZs e entre regiões, evitando falhas de nó único.

7.10 Gerenciamento de atualização

N/A

8 Gerenciamento de permissões do HSS

Se você precisar atribuir permissões diferentes aos funcionários da sua empresa para acessar seus recursos de HSS, o IAM é uma boa opção para o gerenciamento de permissões refinado. O IAM fornece autenticação de identidade, gerenciamento de permissões e controle de acesso, ajudando você a proteger o acesso aos seus recursos de nuvem.

Com o IAM, você pode usar sua conta da Huawei Cloud para criar usuários do IAM para seus funcionários e atribuir permissões aos usuários para controlar seu acesso a tipos de recursos específicos. Por exemplo, alguns desenvolvedores de software em sua empresa precisam usar recursos de HSS, mas não devem excluí-los ou executar operações de alto risco. Para alcançar esse resultado, você pode criar usuários do IAM para os desenvolvedores de software e conceder a eles apenas as permissões necessárias para usar os recursos do HSS.

Se sua conta da Huawei Cloud não precisar de usuários individuais do IAM para gerenciamento de permissões, você poderá pular este capítulo.

O IAM pode ser usado gratuitamente. Você paga apenas pelos recursos na sua conta. Para obter mais informações sobre IAM, consulte **O que é o IAM**?

Permissões do HSS

Por padrão, os novos usuários do IAM não têm permissões atribuídas. Você precisa adicionar um usuário a um ou mais grupos e anexar políticas de permissões ou funções a esses grupos. Os usuários herdam permissões de seus grupos e podem executar operações especificadas em serviços de nuvem.

O HSS é um serviço de nível de projeto implementado e acessado em regiões físicas específicas. Para atribuir permissões do HSS a um grupo de usuários, especifique o escopo como projetos específicos da região e selecione os projetos para que as permissões entrem em vigor. Se **All projects** estiver selecionado, as permissões entrarão em vigor para o grupo de usuários em todos os projetos específicos da região. Ao acessar o HSS, os usuários precisam mudar para uma região onde foram autorizados a usar os serviços em nuvem.

Você pode conceder permissões usando funções ou políticas.

- Funções: um tipo de mecanismo de autorização de alta granularidade que define permissões relacionadas às responsabilidades do usuário. Esse mecanismo fornece apenas um número limitado de funções de nível de serviço para autorização. Algumas funções dependem de outras funções para entrar em vigor. Ao atribuir essas funções aos usuários, lembre-se de atribuir as funções das quais eles dependem. No entanto, as funções não são uma escolha adequada para autorização refinada e controle de acesso seguro.

- Políticas: um tipo de autorização refinada que define as permissões necessárias para executar operações em recursos de nuvem específicos sob determinadas condições. Esse tipo de autorização é mais flexível e ideal para o controle de acesso seguro. Por exemplo, você pode conceder aos usuários do HSS somente as permissões para gerenciar um determinado tipo de recursos. A maioria das políticas define permissões com base em APIs.

A tabela a seguir descreve mais detalhes.

Tabela 8-1 Permissões definidas pelo sistema suportadas por HSS

Nome da função/ política	Descrição	Tipo	Dependência
HSS Administrator	Administrador do HSS, que tem todas as permissões do HSS.	Função definida pelo sistema	• Depende da função **Tenant Guest**. Locatário convidado: uma função global, que deve ser atribuída no projeto global. • Para comprar cotas de proteção do HSS, você deve ter as funções **ECS ReadOnlyAccess**, **BSS Administrator** e **TMS ReadOnlyAccess**. – **ECS ReadOnlyAccess**: permissão de acesso somente leitura para o ECS. Esta é uma política do sistema. – **BSS Administrator**: uma função do sistema, que é o administrador da central de cobrança (BSS) e tem permissões totais para o serviço. – **TMS ReadOnlyAccess**: uma política definida pelo sistema que concede acesso somente leitura ao TMS.
HSSFullAccess	Permissões completas para HSS	Política	Para comprar cotas de proteção do HSS, você deve ter a função **BSS Administrator**. **BSS Administrator**: uma função do sistema, que é o administrador da central de cobrança (BSS) e tem permissões totais para o serviço. **SMN ReadOnlyAccess**: uma política definida pelo sistema que concede acesso somente leitura ao SMN.
HSSReadOnlyAccess	Permissões somente leitura para o HSS.	Política	**SMN ReadOnlyAccess**: uma política definida pelo sistema que concede acesso somente leitura ao SMN.

Referência

- **O que é o IAM?**
- **Criação de um usuário e concessão de permissões**

9 Serviços relacionados

Você pode usar o SMN para receber notificações de alarme, o serviço IAM para gerenciar permissões de usuário e o Cloud Trace Service (CTS) para auditar comportamentos de usuários.

Elastic Cloud Server (ECS)/Bare Metal Server (BMS)

Os agentes do HSS podem ser instalados em ECSs, BMSs ou servidores de terceiros da Huawei Cloud. É aconselhável usar os servidores da Huawei Cloud para uma experiência de serviço melhor e mais confiável.

- Para obter detalhes sobre o ECS, consulte o **Guia de usuário do Elastic Cloud Server**.
- Para obter detalhes sobre o BMS, consulte o **Guia de usuário do Bare Metal Server**.

Cloud Container Engine (CCE)

O CCE pode criar rapidamente um cluster de containers altamente confiável baseado em servidores de nuvem e adicionar nós ao cluster para gerenciamento. O HSS pode instalar o Hostguard-agent nos nós para proteger as aplicações de containers implementadas neles.

NOTA

O CCE é um serviço de alto desempenho e alta confiabilidade por meio do qual as empresas podem gerenciar aplicações em containers. O CCE oferece suporte a aplicações e ferramentas nativas do Kubernetes, permitindo que você configure facilmente um ambiente de tempo de execução de container na nuvem. Para obter mais informações, consulte o *Guia de usuário do Cloud Container Engine*.

Software Repository for Container (SWR)

O SWR fornece gerenciamento fácil, seguro e confiável sobre imagens de containers durante todo o seu ciclo de vida, facilitando a implementação de serviços em containers. Para obter mais informações, consulte o *Guia de usuário do Software Repository for Container*. O HSS verifica vulnerabilidades e configurações em imagens de containers para ajudá-lo a detectar o ambiente de container que não pode ser alcançado pelo software de segurança tradicional.

Simple Message Notification (SMN)

O SMN é um serviço de processamento de mensagens extensível e de alto desempenho.

- Para ativar as notificações de alarme, você deve configurar o SMN primeiro.
- Depois que o SMN estiver ativado, você receberá notificações de alarme enviadas pelo HSS se seu servidor for atacado ou tiver altos riscos detectados.
- Na guia **Alarm Notification**, você pode configurar **Daily Alarm Notification** e **Real-Time Alarm Notification**, conforme necessário.

Para obter detalhes sobre o SMN, consulte *Guia de usuário do Simple Message Notification*.

Identity and Access Management

O IAM é um serviço de gerenciamento de identidade gratuito que pode implementar o isolamento e o controle refinados de permissões de usuários com base nas identidades dos usuários. É o serviço básico de gerenciamento de permissões e pode ser usado gratuitamente.

Para obter detalhes sobre o IAM, consulte *Guia de usuário do Identity and Access Management*.

Cloud Trace Service (CTS)

O CTS é um serviço profissional de auditoria de log que registra as operações do usuário no HSS. Você pode usar os registros para análise de segurança, auditoria de conformidade, rastreamento de recursos e localização de falhas. É o serviço básico de gerenciamento de logs e pode ser usado gratuitamente.

Para obter detalhes sobre o CTS, consulte o *Guia de usuário do Cloud Trace Service*.

10 Conceitos

Quebra de contas

A quebra de conta refere-se ao comportamento do intruso de adivinhar ou quebrar a senha de uma conta.

Senha fraca

Uma senha fraca pode ser facilmente quebrada.

Programa malicioso

Um programa malicioso, como um shell da Web, cavalo de Troia, worm ou vírus, é desenvolvido com ataques ou intenções ilegais de controle remoto.

O malware insere secretamente o código em outro programa para executar programas intrusivos ou perturbadores e danificar a segurança e a integridade dos dados em um servidor infectado. O malware inclui vírus, cavalos de Troia e worms, classificados por suas formas de transmissão.

HSS relata malware identificado e suspeito.

Ransomware

Ransomware surgiu com a economia Bitcoin. É um cavalo de Troia que está disfarçado como um anexo de e-mail legítimo ou software empacotado e engana você para abri-lo ou instalá-lo. Ele também pode chegar em seus servidores por meio de intrusão de site ou servidor.

O ransomware geralmente usa uma variedade de algoritmos para criptografar os arquivos da vítima e exigir o pagamento de um resgate para obter a chave de descriptografia. Moedas digitais como o Bitcoin são normalmente usadas para os resgates, dificultando o rastreamento e a ação judicial contra os invasores.

O ransomware interrompe as empresas e pode causar sérios prejuízos econômicos. Precisamos saber como ele funciona e como podemos evitá-lo.

Autenticação de dois fatores

A autenticação de dois fatores (2FA) refere-se à autenticação do logon do usuário pela combinação da senha do usuário e um código de verificação.

Proteção contra adulteração na Web

Proteção contra adulteração na Web (WTP) é uma edição do HSS que protege seus arquivos, como páginas da Web, documentos e imagens, em diretórios específicos contra adulteração e sabotagem de hackers e vírus.

Cluster

Um cluster consiste em um ou mais ECSs (também conhecidos como nós) na mesma sub-rede. Ele fornece um pool de recursos de computação para executar containers.

Nó

No CGS, cada nó corresponde a um ECS. Os containers são executados em nós.

Imagem

Uma imagem é um sistema de arquivos especial. Ela fornece não apenas programas, bibliotecas, recursos, arquivos de configuração, mas também alguns parâmetros de configuração necessários para um container em execução. Uma imagem do Docker não contém nenhum dado dinâmico, e seu conteúdo permanece inalterado após ser construído.

Container

Um container é a instância de uma imagem e pode ser criado, iniciado, interrompido, excluído e suspenso.

Política de segurança

Uma política de segurança indica a regra de segurança que deve ser seguida para um container em execução. Se um container violar uma política de segurança, uma exceção de container será exibida na página **Runtime Security** do console de gerenciamento de CGS.

Projeto

Os projetos são usados para agrupar e isolar recursos de OpenStack, incluindo recursos de computação, armazenamento e rede. Um projeto pode ser um departamento ou uma equipe de projeto.

Vários projetos podem ser criados para uma conta.

Cota de proteção

Para proteger um servidor, vincule-o a uma cota do HSS.

As cotas das diferentes edições do HSS que você comprou são exibidas no console.

Exemplo:

- Se você tiver comprado uma cota da edição empresarial do HSS, você poderá vinculá-la a um servidor.
- Se você tiver comprado 10 cotas da edição empresarial do HSS, poderá vinculá-las a 10 servidores.

A História de mudanças

Lançado em	Descrição
27/10/2023	Este é o décimo segundo lançamento oficial. Otimização de: ● Monitoramento de métricas em **Monitoramento de riscos** ● Adição de proteção de cluster de container e controle de processo de aplicações em **Edições e recursos**.
25/07/2023	Esta edição é o décimo primeiro lançamento oficial. Adição de: ● 1.8-Declaração de privacidade Otimização de: ● **Edições e recursos**: adição da descrição sobre itens de detecção de intrusão. ● Adição da descrição sobre os SOs suportados pela detecção de vulnerabilidades e correção em **Restrições**.
01/06/2023	Este é o décimo lançamento oficial. Alteração do nome da edição avançada do HSS para edição profissional.
10/12/2022	Este é o nono lançamento oficial. Otimização da descrição da prevenção de ransomware em **Edições e recursos**.
15/11/2022	Este é o oitavo lançamento oficial. Adição das seguintes seções: ● **Segurança**
20/09/2022	Este é o sétimo lançamento oficial. Adição da descrição sobre a compra da edição básica (anual/mensal).
31/08/2022	Este é o sexto lançamento oficial. Modificação da descrição sobre a edição básica. A edição básica pode ser usada gratuitamente dentro de um período específico.

Lançado em	Descrição
15/08/2022	Esta edição é o quinto lançamento oficial. Os seguintes tipos de alarmes são adicionados: ● Programa malicioso ● Exploração de vulnerabilidade comum ● Comportamento anormal do sistema - tarefa crontab suspeita Adição da descrição do recurso de autenticação de dois fatores (2FA). A edição empresarial pode informar alarmes sobre contas não autorizadas.
10/08/2022	Esta edição é o terceiro lançamento oficial. Adição da descrição sobre proteção de aplicações.
28/07/2022	Esta edição é o segundo lançamento oficial. Adição dos sistemas e versões suportados. Para mais detalhes, consulte **SOs suportados**.
30/06/2022	Esta edição é o segundo lançamento oficial. Adição da descrição sobre a estrutura da Web e os recursos de serviço da Web. Adição da descrição sobre o recurso de gerenciamento de vulnerabilidades de aplicações.
30/05/2022	Esta edição é o primeiro lançamento oficial.