Configure uma hora personalizada para downloads de TETRA

Contents

Introduction Informações de Apoio Prerequisites Requirements Componentes Utilizados Configurar Verificar Troubleshoot Informações Relacionadas

Introduction

Este documento descreve como configurar endpoints locais para baixar atualizações TETRA a qualquer momento desejado para atender aos requisitos com uso de largura de banda.

Informações de Apoio

O TETRA é o mecanismo off-line do Secure Endpoint que usa assinaturas de antivírus para fornecer proteção aos endpoints. A TETRA recebe atualizações diárias na sua base de dados de assinaturas para acompanhar todas as novas ameaças em estado selvagem. Essas atualizações podem usar largura de banda significativa em ambientes grandes, portanto, cada endpoint torna aleatório o tempo de download dentro do intervalo de atualização que, por padrão, é definido como 1 hora. Mesmo que diferentes intervalos de atualização estejam disponíveis para escolher na política TETRA, não é possível escolher um horário específico para acionar esse processo de download. Este documento fornece uma solução alternativa para forçar a TETRA a atualizar suas assinaturas AV com trabalhos do Agendamento do Windows.

Prerequisites

Requirements

Conhecimento Básico da configuração de política de Ponto de Extremidade Seguro e dos trabalhos do Agendamento do Windows.

Componentes Utilizados

- Console de nuvem de endpoint seguro
- Conector de ponto de extremidade seguro para Windows 8.1.3
- Windows 10 Enterprise

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

Aviso: conforme descrito na seção de background, as atualizações TETRA podem consumir uma largura de banda significativa. Por padrão, o Secure Endpoint tenta reduzir esse impacto e tornar aleatórias as atualizações TETRA dentro do intervalo de atualização, que é definido como 1 hora por padrão. Não é recomendável forçar todos os conectores a atualizar as definições ao mesmo tempo, especialmente em ambientes grandes. Esse processo deve ser usado somente em situações especiais em que seja crítico controlar o tempo da atualização. Em qualquer outro cenário de caso, as atualizações automáticas são preferíveis.

Escolha uma política de Ponto de Extremidade Seguro para configurar o tempo de download TETRA personalizado.

Observação: lembre-se de que essa configuração é feita com base em políticas e todos os endpoints nessa política são afetados. Portanto, é recomendável colocar todos os dispositivos que você deseja controlar para atualizações TETRA personalizadas na mesma política de endpoint seguro.

Efetue login no Console do Secure Endpoint Management e navegue para **Gerenciamento** > **Políticas**, depois procure a política que você escolheu usar, clique em **editar**. Quando estiver na página de configuração de política, navegue até a **Seção TETRA**. Nesta seção, desmarque a caixa de seleção **Atualizações automáticas de conteúdo** e **salve** a diretiva. Tudo isso está relacionado à configuração no console Secure Endpoint Cloud.

		A	-
_			
-	 		

Name	TETRA-Policy	
Description		
Modes and Engines		
		TETRA ()
Exclusions		Scan Archives
3 exclusion sets		Scan Packed Files ()
Proxy		C Deep Scan Files 0
		Detect Expanded Threat Types 0
		Automatic Content Updates 0
Outbreak Control	Content Update Interval	1 hour v 0
Device Control		Local Server Endersist Lindete Server (1)
Product Updates	Secure Endpoint Update Server	0
Advanced Settings		I Use HTTPS for TETRA Definition Undates
Administrative Features		Secure Endpoint Update Server Configuration
Client User Interface		
File and Process Scan		
Cache		
Endpoint Isolation		
Engines		
TETRA		
Network		

Para a próxima configuração, acesse seu dispositivo Windows e abra um novo arquivo do Bloco de Notas para adicionar estas linhas:

cd C:\Program Files\Cisco\AMP\8.1.3.21242 sfc.exe -forceupdate

Observe que você precisa usar a versão do Secure Endpoint (8.1.3.21242v para este exemplo) que corresponda à versão instalada no momento no endpoint. Se não tiver certeza da versão, você pode clicar no ícone do equipamento da interface do usuário do Secure Endpoint e, em seguida, na guia Statics para verificar a versão atual. Depois de adicionar essas linhas ao bloco de notas, clique em Arquivo e em Salvar como. Em seguida, clique em Salvar como um tipo e selecione Todos os arquivos. Por fim, digite o nome do arquivo e salve-o como extensão .BAT. Se quiser salvar o arquivo na pasta C:\, você precisará executar o notepad com privilégios de Administrador. Como nota lateral, você pode executar o arquivo BAT para forçar a atualização TETRA para como um teste.

Abra o Agendamento de Tarefas Abrir Agendador de Tarefas na máquina com o Windows e clique no botão **Criar uma Tarefa** localizado na coluna direita.

(2) Task Scheduler			-	×
File Action View Help				
🗢 🌩 🔟 🔛 🔟				
Task Scheduler (Local) Task Scheduler Library	Task Scheduler Summary (Last refreshed: 1/24/2023 Overview of Task Scheduler • Overview of Task Scheduler •	Act Tas	tions sk Scheduler (Local) Connect to Another Computer Create Basic Task Create Task	•
	computer will carry out automatically at the times you specify. To begin, click a command in the Δrtinn Task Status	•	Import Task Display All Running Tasks Enable All Tasks History AT Service Account Configuration	
	Status of t Last 24 hours ~ Summary: 0 total - 0 running, 0 succee		View Refresh	•
	Task Name Ri	2	Help	
Create a task from the selected task	Last refreshed at 1/24/2023 6:08:50 PM Refr file.			

Em Guia Geral, digite o nome desta Tarefa e selecione Executar sempre que o usuário estiver conectado ou não. Marque a caixa de seleção Run with the higherst privelages. Na opção configure for, escolha o sistema operacional aplicável. Para esta demonstração, foi usado o Windows 10.

🕒 Create Task		×
General Trigg	gers Actions Conditions Settings	
Name:	TETRA-Update	
Location:	\	
Author:	DESKTOP-00DJGM9\Abraham Barrientos	
Description:		
-Security opt	tions	
When runni	ing the task, use the following user account:	
DESKTOP-0	ODJGM9\Abraham Barrientos Change User or O	Group
O Run only	y when user is logged on	
Run whe	ether user is logged on or not	
🗌 Do n	not store password. The task will only have access to local computer resources.	
Run with	h highest privileges	
Hidden	Configure for: Windows 10	~
	ОК	Cancel

Na guia **Triggers**, clique em **New Trigger**. Na página Nova configuração de gatilho, você pode personalizar o horário em que deseja que o TETRA atualize suas assinaturas. Para este exemplo, foi usada uma programação diária executada às 13:00 hora da máquina local. A opção Data de início define quando esta tarefa se torna ativa. Quando terminar de usar as configurações de agendamento, clique em **ok**.

and a strategy of	On a schodula	
egin the task:	On a schedule	
 One time Daily Weekly Monthly 	Start: 1/24/2023 🖉 1:00: PM 🖨 Synchronize across Recur every: 1 days	time zones
Advanced settir Delay task f	ngs or up to (random delay): 1 hour	
🗌 Repeat task	every: 1 hour v for a duration of: 1 day	~
Stop .	all running tasks at end of repetition duration	
Stop task if	it runs longer than: 3 days 🗸	
Expire: 1/	24/2024 🔍 🗧 6:50:59 PM 🗘 Synchronize across time	zones
Enabled		

Na guia **Actions**, clique em **New Action**. Na guia **Nova ação**, escolha **Iniciar um programa** para a configuração **Ação**. Em Program/Settings (Programas/Configurações), clique em **Browse** (**Procurar**) e pesquise e selecione o script BAT. Clique em **Ok** para criar a ação. Deixe o restante das configurações padrão e clique em **Ok** para criar a Tarefa.

Edit Actio	n	×
You mus	t specify what action this task will perform.	
Action:	Start a program ~	
Progra	m/script:	
"C:\Us	ers\Abraham Barrientos\Desktop\StopService.BAT" Browse	
Add a	rguments (optional):	
Start in	n (optional):	
	OK Cancel	

Finalmente, este Agendador de Tarefas requer credenciais administrativas para criar a tarefa, pois "Executar com privilégios mais altos" foi selecionado. Após a autenticação com credenciais de administrador, a tarefa está pronta para ser executada e executada para informar ao serviço de Ponto de Extremidade Seguro quando atualizar o TETRA de acordo com o agendamento configurado.

Verificar

Clique na pasta **Biblioteca do Agendador de Tarefas** na coluna esquerda. Verifique se o agendamento foi criado e listado como esperado.



Você pode verificar o número de definição TETRA mais recente baixado pelo conector na guia Secure Endpoint User interface > statics. Você pode usar esse número para comparar as definições mais recentes disponíveis no console em Management > Av Definitions summary para descobrir se o dispositivo está atualizado com as definições mais recentes. Outra alternativa é monitorar o valor de "Definições Atualizadas pela Última Vez" para o endpoint específico no Console de Endpoint Seguro.

Hostname	DESKTOP-00DJGM9	Group	Jobarrie_Proxy
Operating System	Windows 10 Enterprise (Build 19045.2486)	Policy	C TETRA-Policy
Connector Version	8.1.3.21242	Internal IP	
Install Date	2023-01-23 13:01:50 CST	External IP	
Connector GUID	22277c92-e5f5-4dcb-894c-392d4428b5c0	Last Seen	2023-01-24 20:24:25 CST
Processor ID	0f8bfbff000006f1	Definition Version	TETRA 64 bit (daily version: 89889)
Definitions Last Updated	2023-01-24 20:24:25 CST	Update Server	tetra-defs.amp.cisco.com
Cisco Secure Client ID	N/A		

Troubleshoot

Quando as definições não são atualizadas como esperado, você pode dar uma olhada nos logs para procurar um erro de atualização de TETRA. Para fazer isso, habilite o modo de depuração na interface de usuário do Secure Endpoint na guia Avançado antes da hora de disparo da tarefa Agendar. Deixe o conector executar nesse modo por pelo menos 20 minutos após o disparador de tarefa de agendamento e examine o arquivo **sfcx.exe.log** mais recente localizado em **C:\Program Files\Cisco\AMP\X.X.X** (onde X.X.X é a versão atual do Secure Endpoint no sistema).

O ForceWakeUpdateThreadAbout nos mostra que o TETRA é acionado pelo nosso Trabalho de Agendamento para atualização conforme esperado. Se esse log não for exibido, pode ser um problema relacionado à configuração da tarefa de agendamento do Windows.

(99070187, +0 ms) Jan 24 20:30:01 [3544]: ForceWakeUpdateThreadAbout to force update thread awake. Forcing tetra def update. (99070187, +0 ms) Jan 24 20:30:01 [1936]: UpdateThread: Tetra ver string retrieved from config: (99070781, +0 ms) Jan 24 20:30:02 [1936]: UpdateTetra entered... (99070781, +0 ms) Jan 24 20:30:02 [1936]: UpdateTetra: elapsed: cur: 1674621002, last: 0,

interval:180

No caso em que a tarefa de agendamento aciona com sucesso o TETRA para atualizar definições, você precisa procurar qualquer erro TETRA relacionado nos logs. Este é um exemplo de um código de erro TETRA 2200, que significa que o serviço foi interrompido durante o processo de atualização. Como solucionar erros gerais de TETRA está fora do escopo deste documento, no entanto, os links no final deste documento são artigos úteis da Cisco sobre solucionar problemas de códigos de erro de TETRA.

ERROR: TetraUpdateInterface::update Update failed with error -2200

Informações Relacionadas

- Troubleshooting de falhas de atualização de definições TETRA
- Cisco Secure Endpoint Falha de Atualização de Definições Tetra com Erro 3000
- Códigos de erro TETRA Windows

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.