

Gerenciar o Nano Server

📅 05/09/2017 ⌚ 23 minutos para ler

Neste artigo

[Usar a comunicação remota do Windows PowerShell](#)

[Usar sessões CIM do Windows PowerShell no WinRM](#)

[Gerenciamento Remoto do Windows](#)

[Executar um rastreamento de rede no Nano Server](#)

[Instalar pacotes de serviço](#)

[Gerenciar atualizações no Nano Server](#)

[Monitoramento de desempenho e eventos no Nano Server](#)

[Usar a configuração de estado desejado do Windows PowerShell com o Nano Server](#)

Aplica-se a: Windows Server 2016

📘 Importante

A partir do Windows Server, versão 1709, o Nano Server estará disponível somente como uma **imagem de sistema operacional base do contêiner**. Confira [Mudanças no Nano Server](#) para saber o que isso significa.

O Nano Server é gerenciado remotamente. Não há nenhum recurso de logon local, nem suporte aos Serviços de Terminal. No entanto, há diversas opções de gerenciamento do Nano Server remotamente, incluindo o Windows PowerShell, WMI (Instrumentação de Gerenciamento do Windows), Gerenciamento Remoto do Windows e EMS (serviços de gerenciamento de emergência).

Para usar qualquer ferramenta de gerenciamento remoto, você provavelmente precisará saber o endereço IP do Nano Server. Algumas formas de descobrir o endereço IP incluem:

- Usar o Console de Recuperação do Nano (confira a seção Usar o Console de Recuperação do Nano Server deste tópico para obter detalhes).
- Conecte o cabo serial ao computador e use EMS.
- Usando o nome do computador atribuído ao Nano Server durante a configuração, você pode obter o endereço IP com ping. Por exemplo, `ping NanoServer-PC /4`.

Usar a comunicação remota do Windows PowerShell

Para gerenciar o Nano Server com a comunicação remota do Windows PowerShell, é necessário adicionar o endereço IP do Nano Server à lista de hosts confiáveis do seu computador de

gerenciamento, adicionar a conta que você está usando para os administradores do Nano Server e ativar o CredSSP se quiser usar esse recurso.

⚠ Observação


Se o Nano Server de destino e o computador de gerenciamento estiverem na mesma floresta do AD DS (ou em florestas com uma relação de confiança), você não deverá adicionar o Nano Server à lista de hosts confiáveis -- você pode se conectar ao Nano Server usando seu nome de domínio totalmente qualificado, por exemplo: PS C:> Enter-PSSession -ComputerName nanoserver.contoso.com -Credential (Get-Credential)

Para adicionar o Nano Server à lista de hosts confiáveis, execute este comando em um prompt com privilégios elevados do Windows PowerShell:

```
Set-Item WSMan:\localhost\Client\TrustedHosts "<IP address of Nano Server>"
```

Para iniciar a sessão remota do Windows PowerShell, inicie uma sessão local do Windows PowerShell com privilégios elevados e execute estes comandos:

```
$ip = "\<IP address of Nano Server>"
$user = "$ip\Administrator"
Enter-PSSession -ComputerName $ip -Credential $user
```

 Copiar

Agora você pode executar comandos do Windows PowerShell no Nano Server normalmente.

⚠ Observação

Nem todos os comandos do Windows PowerShell estão disponíveis nesta versão do Nano Server. Para ver quais estão disponíveis, execute `Get-Command -CommandType Cmdlet`

Parar a sessão remota com o comando `Exit-PSSession`

Usar sessões CIM do Windows PowerShell no WinRM

Você pode usar sessões e instâncias CIM no Windows PowerShell para executar comandos WMI no Windows Remote Management (WinRM).

Inicie a sessão CIM executando estes comandos em um prompt do Windows PowerShell:

 Copiar

```
$ip = "<IP address of the Nano Server>"
$ip\Administrator
$cim = New-CimSession -Credential $user -ComputerName $ip
```

Com a sessão estabelecida, você pode executar vários comandos WMI, por exemplo:

```
Get-CimInstance -CimSession $cim -ClassName Win32_ComputerSystem | Format-List *
Get-CimInstance -CimSession $Cim -Query "SELECT * from Win32_Process WHERE name LIKE 'p%'"
```

 Copiar

Gerenciamento Remoto do Windows

Você pode executar programas remotamente no Nano Server com o WinRM (Gerenciamento Remoto do Windows). Para usar o WinRM, primeiro configure o serviço e defina a página de código com estes comandos em um prompt de comandos com privilégios elevados:

winrm quickconfig

winrm set winrm/config/client @{TrustedHosts="<endereço ip do Nano Server>"}

chcp 65001

Agora você pode executar comandos remotamente no Nano Server. Por exemplo:

winrs -r:<endereço IP do Nano Server> -u:Administrator -p:<senha de administrador do Nano Server> ipconfig

Para saber mais sobre o Gerenciamento Remoto do Windows, confira [Visão geral do WinRM \(Gerenciamento Remoto do Windows\)](#).

Executar um rastreamento de rede no Nano Server

Rastreamento de netsh, Tracelog.exe e Logman.exe não estão disponíveis no Nano Server. Para capturar os pacotes de rede, você pode usar estes cmdlets do Windows PowerShell:

```
New-NetEventSession [-Name]
Add-NetEventPacketCaptureProvider -SessionName
Start-NetEventSession [-Name]
Stop-NetEventSession [-Name]
```

 Copiar

Esses cmdlets estão documentados com detalhes em [Cmdlets de captura de pacote de evento de rede do Windows PowerShell](#)

Instalar pacotes de serviço

Se você quiser instalar pacotes de serviço, use o parâmetro `-ServicingPackagePath` (você pode passar uma matriz de caminhos para arquivos `.cab`):

```
New-NanoServerImage -DeploymentType Guest -Edition Standard -MediaPath \\Path\To\Media\en_us -BasePath
.\Base -TargetPath .\NanoServer.wim -ServicingPackagePath \\path\to\kb123456.cab
```

Geralmente, um pacote de serviço ou hotfix é baixado como um item de KB que contém um arquivo `.cab`. Execute estas etapas para extrair o arquivo `.cab`, que pode ser instalado com o parâmetro `-ServicingPackagePath`:

1. Baixe o pacote de serviço (do artigo da Base de Dados de Conhecimento associado ou do [Catálogo do Microsoft Update](#)). Salve-o em um compartilhamento de rede ou diretório local, por exemplo: `C:\ServicingPackages`
2. Crie uma pasta na qual você salvará o pacote de serviço extraído. Exemplo: `c:\KB3157663_expanded`
3. Abra um console do Windows PowerShell e use o comando `Expand` especificando o caminho até o arquivo `.msu` do pacote de serviço, incluindo o parâmetro `-f:*` e o caminho onde você deseja que o pacote de serviço seja extraído. Por exemplo:

```
Expand "C:\ServicingPackages\Windows10.0-KB3157663-x64.msu" -f:* "C:\KB3157663_expanded"
```

Os arquivos expandidos devem ser semelhantes a este:

```
C:>dir C:\KB3157663_expanded
```

O volume da unidade C é o sistema operacional

O Número de série do volume é B05B-CC3D

Diretório de `C:\KB3157663_expanded`

```
04/19/2016 01:17 PM <DIR> .
```

```
04/19/2016 01:17 PM <DIR> ..
```

```
04/17/2016 12:31 AM 517 Windows10.0-KB3157663-x64-pkgProperties.txt
```

```
04/17/2016 12:30 AM 93,886,347 Windows10.0-KB3157663-x64.cab
```

```
04/17/2016 12:31 AM 454 Windows10.0-KB3157663-x64.xml
```

```
04/17/2016 12:36 AM 185,818 WSUSSCAN.cab
```

```
4 File(s) 94,073,136 bytes
```

```
2 Dir(s) 328,559,427,584 bytes free
```

4. Execute `New-NanoServerImage` com o parâmetro `-ServicingPackagePath` apontando para o arquivo `.cab` nesse diretório, por exemplo:

```
New-NanoServerImage -DeploymentType Guest -Edition Standard -MediaPath
\\Path\To\Media\en_us -BasePath .\Base -TargetPath .\NanoServer.wim -ServicingPackagePath
C:\KB3157663_expanded\Windows10.0-KB3157663-x64.cab
```

Gerenciar atualizações no Nano Server

No momento, você pode usar o provedor do Windows Update para a WMI (Instrumentação de Gerenciamento do Windows) a fim de localizar a lista de atualizações aplicáveis e então instalar todos ou um subconjunto delas. Se você usar o WSUS (Windows Server Update Services), também poderá configurar o Nano Server para contatar o servidor do WSUS a fim de obter atualizações.

Em todos os casos, primeiro estabeleça uma sessão remota do Windows PowerShell para o computador do Nano Server. Esses exemplos usam `$sess` para a sessão; se você estiver usando alguma outra coisa, substitua esse elemento conforme o necessário.

Ver todas as atualizações disponíveis

Obtenha a lista completa de atualizações aplicáveis com estes comandos:

 Copiar

```
$sess = New-CimInstance -Namespace root/Microsoft/Windows/WindowsUpdate -ClassName MSFT_WUOperationsSession

$scanResults = Invoke-CimMethod -InputObject $sess -MethodName ScanForUpdates -Arguments @{"SearchCriteria"="IsInstalled=0";OnlineScan=$true}
```

Observação:

Se não houver atualização disponível, esse comando retornará o seguinte erro:

 Copiar

```
Invoke-CimMethod : A general error occurred that is not covered by a more specific error code.

At line:1 char:16

+ ... anResults = Invoke-CimMethod -InputObject $sess -MethodName ScanForUp ...
+
+ ~~~~~
+ CategoryInfo          : NotSpecified: (MSFT_WUOperatio...-5b842a3dd45d")
:CimInstance) [Invoke-CimMethod], CimException

+ FullyQualifiedErrorId : MI RESULT 1,Microsoft.Management.Infrastructure.
CimCmdlets.InvokeCimMethodCommand
```

Instalar todas as atualizações disponíveis

Você pode detectar, baixar e instalar **todas** as atualizações disponíveis ao mesmo tempo usando estes comandos:



```
$sess = New-CimInstance -Namespace root/Microsoft/Windows/WindowsUpdate -ClassName MSFT_WUOperationsSession

$scanResults = Invoke-CimMethod -InputObject $sess -MethodName ApplyApplicableUpdates

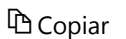
Restart-Computer
```

Observação:

O Windows Defender impedirá a instalação das atualizações. Para contornar esse problema, desinstale o Windows Defender, instale as atualizações e, em seguida, reinstale o Windows Defender. Como alternativa, você pode baixar as atualizações em outro computador, copiá-las no Nano Server e, em seguida, aplicá-las com DISM.exe.

Verificar a instalação das atualizações

Use estes comandos para obter uma lista das atualizações instaladas no momento:



```
$sess = New-CimInstance -Namespace root/Microsoft/Windows/WindowsUpdate -ClassName MSFT_WUOperationsSession

$scanResults = Invoke-CimMethod -InputObject $sess -MethodName ScanForUpdates -Arguments @{SearchCriteria="IsInstalled=1";OnlineScan=$true}
```

Observação:

Esses comandos listam o que está instalado, mas não citam especificamente "instalado" na saída. Se você precisar que a saída inclua isso, por exemplo em um relatório, execute



```
Get-WindowsPackage -Online
```

Usar o WSUS

Os comandos listados acima consultarão os serviços Windows Update e Microsoft Update na Internet para localizar e baixar atualizações. Se você usar o WSUS, poderá configurar chaves do Registro no Nano Server para usar o servidor WSUS.

Confira a tabela "Windows Update Agent Environment Options Registry Keys" (Chaves do Registro de opções de ambiente do agente do Windows Update) em [Configure Automatic Updates in a Non-Active Directory Environment \(Configurar atualizações automáticas em um ambiente que não é do Active Directory\)](#).

Defina pelo menos as chaves do Registro **WUServer** e **WUStatusServer**, mas dependendo de como você implementou o WSUS, outros valores podem ser necessários. Você sempre pode confirmar essas configurações examinando outro Windows Server no mesmo ambiente.

Depois de definir esses valores para o WSUS, os comandos na seção acima consultarão esse servidor em busca de atualizações e usarão a origem do download.

Atualizações Automáticas

Atualmente, a maneira de automatizar a instalação da atualização é converter as etapas acima em um script do Windows PowerShell local e, em seguida, criar uma tarefa agendada para executá-lo e reiniciar o sistema em sua agenda.

Monitoramento de desempenho e eventos no Nano Server

O Nano Server é totalmente compatível com a estrutura do ETW ([Rastreamento de Eventos para Windows](#)), mas algumas ferramentas conhecidas, usadas para gerenciar o rastreamento e contadores de desempenho, não estão disponíveis atualmente no Nano Server. No entanto, o Nano Server tem ferramentas e cmdlets para realizar cenários mais comuns de análise de desempenho.

O fluxo de trabalho de alto nível permanece o mesmo em qualquer instalação do Windows Server - o rastreamento de baixa sobrecarga é executado no computador de destino (Nano Server) e os arquivos de rastreamento e/ou logs resultantes são processados posteriormente offline em um computador separado, usando ferramentas como o [Analisador de Desempenho do Windows](#), [Analisador de Mensagem](#) ou outros.


⚠ Observação

Veja [Como copiar arquivos do Nano Server](#) para ter uma atualização sobre como transferir arquivos usando a comunicação remota do PowerShell.


As seções a seguir listam as atividades de coleta de dados de desempenho mais comuns, juntamente com uma forma com suporte de realizá-las no Nano Server.

Consultar os provedores de eventos disponíveis

[Windows Performance Recorder](#) é a ferramenta para consultar os provedores de eventos disponíveis da seguinte maneira:

	 Copiar
<pre>wpr.exe -providers</pre>	


Você pode filtrar a saída para os tipos de eventos de seu interesse. Por exemplo:

	 Copiar
<pre>PS C:\> wpr.exe -providers select-string "Storage"</pre>	
595f33ea-d4af-4f4d-b4dd-9dacdd17fc6e	: Microsoft-
Windows-StorageManagement-WSP-Host	
595f7f52-c90a-4026-a125-8eb5e083f15e	: Microsoft-
Windows-StorageSpaces-Driver	
69c8ca7e-1adf-472b-ba4c-a0485986b9f6	: Microsoft-
Windows-StorageSpaces-SpaceManager	
7e58e69a-e361-4f06-b880-ad2f4b64c944	: Microsoft-
Windows-StorageManagement	
88c09888-118d-48fc-8863-e1c6d39ca4df	: Microsoft-
Windows-StorageManagement-WSP-Spaces	

Rastreamentos de registro de um único provedor ETW

Você pode usar os novos [cmdlets de Gerenciamento de Rastreamento de Evento](#) para isso. Veja um exemplo de fluxo de trabalho:


Crie e inicie o rastreamento, especificando um nome de arquivo para armazenar os eventos.

	 Copiar
<pre>PS C:\> New-EtwTraceSession -Name "ExampleTrace" -LocalFilePath c:\etrace.etl</pre>	

Adicione um provedor de GUID ao rastreamento. Use `wpr.exe -providers` para o Nome do Provedor para conversão de GUID.

	 Copiar
<pre>PS C:\> wpr.exe -providers select-string "Kernel-Memory"</pre>	
d1d93ef7-e1f2-4f45-9943-03d245fe6c00	: Microsoft-
Windows-Kernel-Memory	
<pre>PS C:\> Add-EtwTraceProvider -Guid "{d1d93ef7-e1f2-4f45-9943-03d245fe6c00}" -SessionName "ExampleTrace"</pre>	

Remover o rastreamento - isso interrompe a sessão de rastreamento, liberando os eventos para o arquivo de log associado.

	 Copiar
<pre>PS C:\> Remove-EtwTraceSession -Name "ExampleTrace"</pre>	


```
PS C:\> dir .\etrace.etl
```

```
Directory: C:\
```

Mode	LastWriteTime	Length	Name
----	-----	-----	----
-a----	9/14/2016 11:17 AM	16515072	etrace.etl

❗ Observação

Este exemplo mostra como adicionar um provedor de rastreamento único à sessão, mas você também pode usar o cmdlet `Add-EtwTraceProvider` várias vezes em uma sessão de rastreamento com GUIDs de provedor diferentes a fim de habilitar o rastreamento de várias fontes. Outra alternativa é usar os perfis `wpr.exe` descritos abaixo.

Rastreamentos de registro de um vários provedores ETW

A opção `-profiles` de [Windows Performance Recorder](#) habilita o rastreamento de vários provedores ao mesmo tempo. Há uma série de perfis internos como CPU, Rede e DiskIO para escolher:



```
PS C:\Users\Administrator\Documents> wpr.exe -profiles
```

```
Microsoft Windows Performance Recorder Version 10.0.14393 (CoreSystem)  
Copyright (c) 2015 Microsoft Corporation. All rights reserved.
```

GeneralProfile	First level triage
CPU	CPU usage
DiskIO	Disk I/O activity
FileIO	File I/O activity
Registry	Registry I/O activity
Network	Networking I/O activity
Heap	Heap usage
Pool	Pool usage
VirtualAllocation	VirtualAlloc usage
Audio	Audio glitches
Video	Video glitches
Power	Power usage
InternetExplorer	Internet Explorer
EdgeBrowser	Edge Browser
Minifilter	Minifilter I/O activity
GPU	GPU activity
Handle	Handle usage
XAMLActivity	XAML activity
HTMLActivity	HTML activity
DesktopComposition	Desktop composition activity
XAMLAppResponsiveness	XAML App Responsiveness analysis
HTMLResponsiveness	HTML Responsiveness analysis
ReferenceSet	Reference Set analysis

ResidentSet	Resident Set analysis
XAMLHTMLAppMemoryAnalysis	XAML/HTML application memory analysis
UTC	UTC Scenarios
DotNET	.NET Activity
WdfTraceLoggingProvider	WDF Driver Activity

Para obter orientações detalhadas sobre a criação de perfis personalizados, confira a [documentação do WPR.exe](#).

Registrar rastreamentos ETW durante o momento de inicialização do sistema operacional

Use o cmdlet `New-AutoLoggerConfig` para coletar eventos durante a inicialização do sistema. O uso é muito semelhante ao do cmdlet `New-EtwTraceSession`, mas os provedores adicionados à configuração do Autologger serão habilitados somente no início na próxima inicialização. O fluxo de trabalho geral tem esta aparência:

Primeiro, crie uma nova configuração de Autologger.

Copiar

```
PS C:\> New-AutoLoggerConfig -Name "BootPnpLog" -LocalFilePath c:\bootpnp.etl
```

Adicione um provedor ETW a ela. Este exemplo usa o provedor de Kernel PnP. Invoque `Add-EtwTraceProvider` novamente, especificando o mesmo nome de Autologger, mas um GUID diferente para habilitar a coleta de rastreamento de inicialização de várias fontes.

Copiar

```
Add-EtwTraceProvider -Guid "{9c205a39-1250-487d-abd7-e831c6290539}" -AutologgerName BootPnpLog
```

Isso não inicia uma sessão do ETW imediatamente, mas em vez disso, configura uma para iniciar na próxima inicialização. Após a reinicialização, uma nova sessão do ETW com o nome da configuração do Autologger será iniciada automaticamente com os provedores de rastreamento adicionados habilitados. Após a inicialização do Nano Server, o comando a seguir interromperá a sessão de rastreamento depois de liberar os eventos registrados para o arquivo de rastreamento associado:

Copiar

```
PS C:\> Remove-EtwTraceSession -Name BootPnpLog
```

Para evitar que outra sessão de rastreamento seja criada automaticamente na próxima inicialização, remova a configuração de Autologger da seguinte maneira:

```
PS C:\> Remove-AutologgerConfig -Name BootPnpLog
```

Para coletar rastreamentos de inicialização e instalação em um número de sistemas, ou em um sistema sem disco, considere o uso da [Coleta de evento de configuração e inicialização](#).

Capturar dados do contador de desempenho

Normalmente, você monitora os dados do contador de desempenho com o GUI de Perfmon.exe. No Nano Server, use o equivalente de linha de comando de `Typeperf.exe`. Por exemplo:

Consulta contadores disponíveis – você pode filtrar a saída para localizar facilmente os que são de seu interesse.

```
PS C:\> typeperf.exe -q | Select-String "UDpv6"

\UDpv6\Datagrams/sec
\UDpv6\Datagrams Received/sec
\UDpv6\Datagrams No Port/sec
\UDpv6\Datagrams Received Errors
\UDpv6\Datagrams Sent/sec
```

As opções permitem que você especifique o número de vezes e o intervalo no qual os valores de contador são coletados. No exemplo abaixo, o Tempo Ocioso do Processador é coletado cinco vezes a cada três segundos.

```
PS C:\> typeperf.exe "\Processor Information(0,0)\% Idle Time" -si 3 -sc 5

"(PDH-CSV 4.0)","\\ns-g2\Processor Information(0,0)\% Idle Time"
"09/15/2016 09:20:56.002","99.982990"
"09/15/2016 09:20:59.002","99.469634"
"09/15/2016 09:21:02.003","99.990081"
"09/15/2016 09:21:05.003","99.990454"
"09/15/2016 09:21:08.003","99.998577"
Exiting, please wait...
The command completed successfully.
```

Outras opções de linha de comando permitem que você especifique nomes de contador de desempenho de interesse em um arquivo de configuração, redirecionando a saída para um arquivo de log, entre outras coisas. Veja a [documentação sobre typeperf.exe](#) para obter detalhes.

Você também pode usar a interface gráfica do Perfmon.exe remotamente com destinos do Nano Server. Ao adicionar contadores de desempenho ao modo de exibição, especifique o destino do Nano Server no

nome do computador em vez do padrão .

Interagir com o Log de eventos do Windows

O Nano Server oferece suporte ao cmdlet `Get-WinEvent`, que fornece recursos de filtragem e consulta do Log de eventos do Windows, tanto localmente como em um computador remoto. Encontre opções detalhadas e exemplos na [página de documentação do Get-WinEvent](#). Este exemplo simples recupera os *Erros* indicados no log *Sistema* durante os últimos dois dias.

 Copiar

```
PS C:\> $StartTime = (Get-Date) - (New-TimeSpan -Day 2)
PS C:\> Get-WinEvent -FilterHashTable @{LogName='System'; Level=2; StartTime=$StartTime} |
select TimeCreated, Message

TimeCreated          Message
-----
9/15/2016 11:31:19 AM Task Scheduler service failed to start Task Compatibility module.
Tasks may not be able to reg...
9/15/2016 11:31:16 AM The Virtualization Based Security enablement policy check at phase 6
failed with status: {File...
9/15/2016 11:31:16 AM The Virtualization Based Security enablement policy check at phase 0
failed with status: {File...
```

O Nano Server também oferece suporte a `wevtutil.exe` que permite recuperar informações sobre os logs de eventos e editores. confira [documentação do wevtutil.exe](#) para obter mais detalhes.

Ferramentas de interface gráfica

As [ferramentas de gerenciamento de servidor baseadas na Web](#) podem ser usadas para gerenciar remotamente os destinos do Nano Server e apresentar um Log de eventos do Nano Server usando um navegador da Web. Por fim, o snap-in MMC Visualizador de Eventos (eventvwr.msc) também pode ser usado para exibir logs- - basta abri-lo em um computador com uma área de trabalho e apontá-lo para um Nano Server remoto.

Usar a configuração de estado desejado do Windows PowerShell com o Nano Server

É possível gerenciar o Nano Server como nós de destino com a Configuração de Estado Desejado (DSC) do Windows PowerShell. No momento, só é possível gerenciar nós que estejam executando o Nano Server com DSC no modo push. Nem todos os recursos de DSC funcionam com o Nano Server.

Para obter mais detalhes, confira [Usar DSC no Nano Server](#).