Boas Práticas

Gerenciamento de Patches

N-able N-sight RMM

Sumário

Introdução

Este documento tem como objetivo abordar a implementação do Gerenciamento de Patches de forma segura e evitando erros, bem como fornecer familiaridade com a ferramenta e os conceitos envolvidos.

Como qualquer outra solução, a implementação do **Gerenciamento de Patches** exige planejamento e compreensão do ambiente e da ferramenta.

É necessário que você, seja prestador de serviço ou possua TI interna, entenda que o **Gerenciamento de Patches** envolve uma série de responsabilidade como acompanhamento, gestão e manutenção das atualizações, aprovações e instalações.

Vale ressaltar também a importância dos relatórios do recurso para a gestão e acompanhamento diário.

Queremos sua opinião! Ajude-nos a aprimorar este documento. Qualquer dúvida, crítica ou sugestão, por favor, encaminhe um e-mail para **boaspraticas@addee.com.br**.

1. Conceito

+ O que é Patch e qual a importância do seu gerenciamento?

Em uma tradução literal do inglês, “patch” significa remendo e, basicamente, são as atualizações lançadas pelo fornecedor de software que tem a função de auxiliar no combate às vulnerabilidades dos programas e na correção do controle do hardware, de modo a corrigir erros e falhas, além de melhorar sua usabilidade.

O **Gerenciamento de Patches** consiste na tarefa de gerenciar os patches disponíveis, alocar as correções para os programas, ajustar as instalações e documentar os procedimentos executados.

+ Devemos aprovar e instalar todos os patches detectados?

O **Gerenciamento de Patches** não serve apenas para realizar uma atualização constante de softwares, e sim uma gestão consciente, visando o pleno funcionamento do ambiente de TI do cliente com segurança e estabilidade.

Recomendamos que você analise e entenda o conteúdo relacionado ao patch antes de aplicá-lo.

Sugerimos também ter um ambiente de testes, onde você possa avaliar os patches antes de aplicá-los no ambiente do cliente.

Para patches cuja a gravidade é crítica, recomendamos que a aprovação e instalação sejam feitas de forma automática.

Esta metodologia pode ser trabalhosa e demandar bastante tempo, porém esta rotina vai prevenir problemas ainda maiores relacionados à segurança e estabilidade do sistema.

+ O GP também gerencia atualizações de softwares terceiros?

SIM! A ferramenta fornece uma solução eficaz, não apenas para os patches de segurança dos aplicativos Microsoft Windows e Office, como também outros aplicativos de uso comum, como o Adobe Reader, Google Chrome, Java, entre outros.

Através **deste link** é possível ter acesso a todas as aplicações suportadas pela nossa solução.

Lembrando que a **N-able** sempre acrescenta novas aplicações de tempos em tempos, portanto se a sua aplicação ainda não consta na lista é provável que em breve passará a ter compatibilidade.

E para os softwares de terceiros que ainda não são suportados pela solução, a atualização dos mesmos deve ser realizada manualmente, pelo próprio software.

+ Como decidir quando agendar uma atualização pelo GP?

Vamos abordar as principais tarefas do processo de aplicação de patches e como agendá-las:

- **Verificação / Detecção de Patches**

Podemos pensar que a aplicação de patches de forma semanal ou mesmo mensal são suficientes. Então, por que devemos considerar fazer estas verificações diariamente?

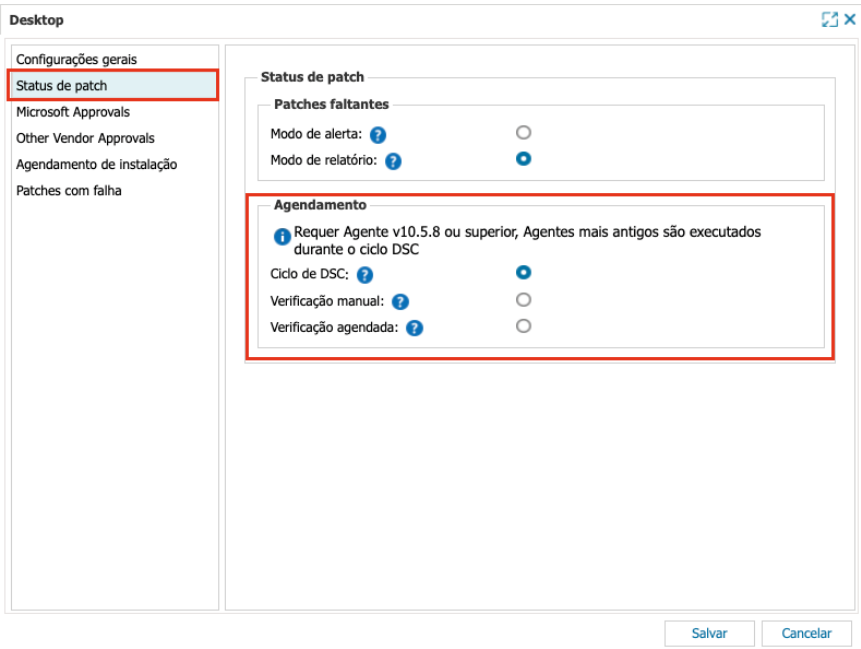
Existem três razões principais para aumentar esta frequência:

1. **Visibilidade** – saber o que é necessário em tempo real sempre que o cliente entra em contato.

2. **Correções de emergência** – Algumas correções precisam ser instaladas fora do cronograma regular, e devido a urgência destas correções não é viável aguardar o próximo agendamento.

3. **Microsoft AV incorporado** – são lançadas atualizações com muita frequência. Se os teus clientes utilizam esta solução, instale as atualizações à medida que forme publicadas.

Recomendamos fazer a verificação de patches através da "**Verificação Diária de Segurança (DSC)**", para que você possa identificar novos patches com maior frequência, tendo assim um ambiente mais seguro e estável.



- **Aprovar patches (manual ou automaticamente)**

É comum aprovar todos os patches manualmente. Se isto funciona para você, faça-o pelo menos quinzenalmente, devido ao risco do ambiente estar vulnerável, pois é sabido que um cyber atacante pode desenvolver uma ameaça para uma vulnerabilidade em média de 15 dias.

Também recomendamos que aprove e instale automaticamente as atualizações de definição para o Microsoft Defender (o antivírus gratuito da Microsoft), caso o cliente o utilize.

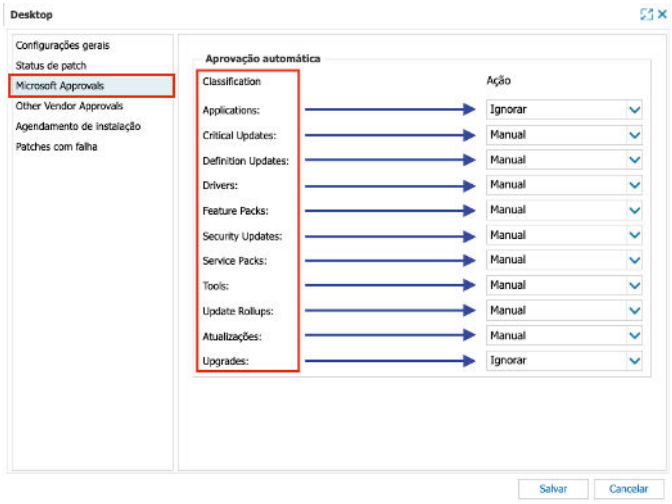
Agora, se você deseja aprovar alguns patches automaticamente (com ou sem atraso), normalmente são aprovados automaticamente apenas os patches de segurança e críticos. O restante pode ser revisado manualmente.

Por fim, pode ser aprovado tudo automaticamente. Isto pode ser agressivo, mas se funcionar em seu ambiente, então ótimo. Independente de aprovar os patches manualmente ou automaticamente, recomendamos seguir estes três princípios abaixo:

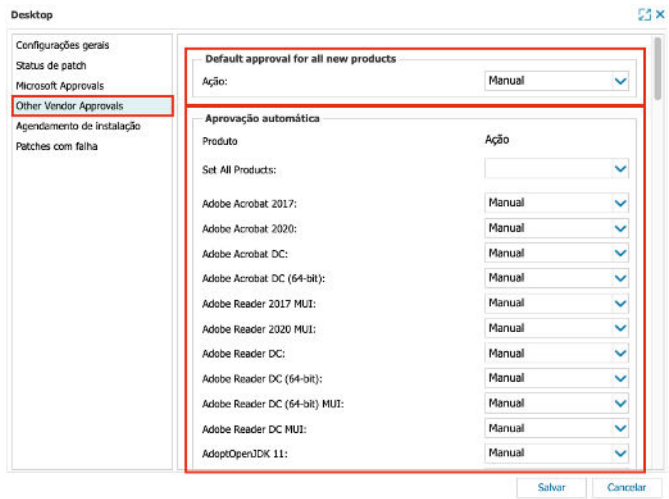
1. **Não deixe patches não aprovados** – aprove-os, recuse-os ou marque-os como ignorados, para garantir que você tenha um relatório limpo para análise.

2. **Faça a busca com frequência** – verifique pelo menos semanalmente. Quarta-feira é, no geral, um bom dia para realizar esta busca por novos patches, pois a maioria sempre é liberada na Terça-feira.

3. **Escreva um procedimento padrão** – um procedimento padrão, um passo a passo, ou até mesmo uma "receita de bolo", permite que qualquer pessoa da sua equipe possa fazer a aprovação/recusa de maneira confiável e consistente, pois o processo permanece o mesmo.



Aprovação – Microsoft



Aprovação – Softwares de Terceiros

- **Instalando patches**

Nas estações de trabalho recomendamos a instalação dos patches durante o dia.

Você pode instalar o patches semanalmente, ou em um dia de sua escolha, e configurá-los para corrigir na próxima vez que o dispositivo for reiniciado, caso perca a sua janela de instalação.

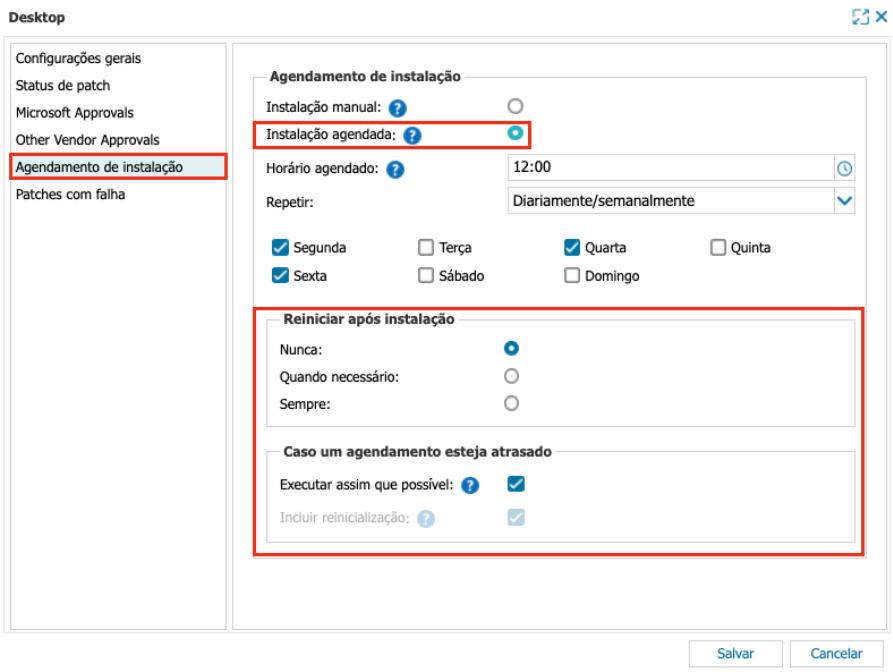
Também pode instalar os patches por volta do horário do almoço (entre 11:30h e 13:00h, por exemplo), todos os dias, para minimizar possíveis interrupções.

Também pode instalá-los mais tarde, quando o usuário não estiver mais a frente do dispositivo (este, porém, precisará estar ligado para que a instalação ocorra).

- **Reiniciar o dispositivo após a instalação dos patches**

A reinicialização é complicada, pois afetará o usuário.

Para evitar este problema você pode agendar uma reinicialização forçada uma vez por semana, à noite, se os dispositivos estiverem online.



2. Funcionamento

Quando o **Gerenciamento de Patches** é ativado em um device, o agente assume as configurações de atualização do Windows Update. Assim, as atualizações do Windows são aprovadas e recusadas somente através do recurso do **N-sight RMM**.

Importante: **Como o mecanismo do Gerenciamento de Patches assume o controle administrativo do Windows Update para baixar arquivos e instalar os patches, caso o serviço do Windows Update seja desabilitado, o Gerenciamento de Patches não receberá mais nenhum patch disponibilizado pela Microsoft para realizar seu gerenciamento.**

O **Gerenciamento de Patches** utiliza o **Windows Update Agent (WUA)** e gerencia as instalações dos patches do tipo "B". Lançados na **"Patch Tuesday"** (lançamento normalmente realizado na segunda terça-feira do mês, os patches do tipo **"B"** são considerados como as atualizações mais importantes.

Eles incluem novas correções de segurança, correções de atualizações anteriores e correções de bugs lançadas anteriormente nas atualizações de tipo **"C"** e **"D"**. Atualizações do tipo **"C"** e **"D"** são consideradas atualizações opcionais, portanto elas são consideradas pela Microsoft como versões de "preview releases".

Assim, elas não são adicionadas nas instalações automáticas do Windows Update. As atualizações do tipo **"C"** e **"D"** estão focadas em novas correções de bugs e melhorias para problemas **"non-security"**. Desta forma, elas não estão inclusas em nenhuma atualização de segurança.

Como a ferramenta visa priorizar o pleno funcionamento do ambiente TI com segurança e estabilidade, as atualizações do tipo **"C"** e **"D"** não são listadas pela ferramenta.

Através **deste artigo** da Microsoft você terá mais detalhes sobre este assunto. E através **deste site** você terá acesso ao catálogo de **KBs**, disponibilizadas pela Microsoft.

Observação: Os Sistemas Operacionais descontinuados (tais como Windows 7 pré-SP1, Windows Server 2008 pré-R2, por já estarem descontinuados pelo próprio fabricante (Microsoft, não são compatíveis com o mecanismo de gerenciamento de patches. Os usuários utilizando Sistemas Operacionais Windows que foram descontinuados, precisarão ter em mente de que estão correndo um grande risco de segurança.

3. Concentrador de Sites

O **Concentrador de Sites** é usado para reduzir o tráfego da rede externa, baixando e armazenando em cache os arquivos de instalações e atualizações não somente relacionados aos patches, mas também a todos os recursos do **N-sight RMM** (antivírus, acesso remoto, backup, etc.), tudo em um local centralizado (servidor).

Então, os demais dispositivos deste site (estações de trabalho ou outros servidores) buscarão os arquivos de atualização no cache deste servidor designado como **Concentrador de Sites**, garantindo que cada arquivo seja baixado apenas uma vez naquela rede ou infraestrutura.

Se houver um firewall no servidor (que foi designado como concentrador) ou na rede, é preciso criar uma regra que permita o acesso através da **porta 8123** (esta é a porta padrão do concentrador, mas ela pode ser alterada), pois todos os dispositivos do site precisarão ter acesso ao servidor através desta porta.

Recomendamos que este recurso seja aplicado a qualquer infraestrutura com **mais de 10 dispositivos**, sendo necessário que exista ao menos 1 servidor dentre estes (pois o servidor normalmente permanece ativo por bastante tempo). Isto contribuirá, de forma significativa, na performance e na otimização de banda de internet.

Observações: O **Concentrador de Sites** tem como objetivo, único e exclusivo, realizar download de patches e atualizações dos recursos citados acima. Nenhum outro tipo de download será feito através dele, assim como nenhum tipo de upload do agente dos dispositivos.

+ Como funciona o Concentrador de Sites em diferentes cenários?

Se você tiver um **Concentrador de Sites** configurado em um local, pode haver momentos em que esse dispositivo não esteja acessível à Internet ou tenha alguns problemas de comunicação.

Se for esse o caso, após uma tentativa inicial do agente do **N-sight RMM** de baixar e instalar patches por meio do **Concentrador**, ele retornará diretamente ao fornecedor, como qualquer outro agente faz se nenhum **Concentrador** estiver presente.

Certifique-se de verificar nossa KB sobre como configurar um **Concentrador de Sites neste link**.

Existem mais algumas considerações, especialmente se um **Concentrador** estiver sendo usado e você gerenciar todos os tipos de patches. Por padrão, agindo como um proxy de cache, o **Concentrador** lerá e armazenará em cache apenas patches HTTP.

Para armazenar em cache os downloads HTTPS, em teoria, seria necessário armazenar um certificado raiz personalizado nesse dispositivo. A maioria dos patches do Windows são apenas HTTP e serão armazenados em cache pelo **Concentrador**, mas a maioria dos patches de terceiros são HTTPS e não serão armazenados em cache. Considere isso, especialmente ao configurar seu cronograma de download e instalação de terceiros.

Também existe a possibilidade de alterar o intervalo de cache padrão do **Concentrador de Sites**. Isso pode ser conseguido através do nosso recurso de fundo remoto, conforme descrito abaixo.

Acesse o **System Shell** e execute os seguintes comandos:

- .. reg add HKLM\SOFTWARE\drydock /v DefaultCacheInterval /t REG_DWORD/d 604800 /f
- .. net stop svcDrydock
- .. net start svcDrydock

Estes comandos foram extraídos das seguintes páginas do **Microsoft TechNet**:

- **https://technet.microsoft.com/en-us/library/cc742162(v=ws.11).aspx**
- **https://technet.microsoft.com/en-in/library/cc736564(v=ws.10).aspx**

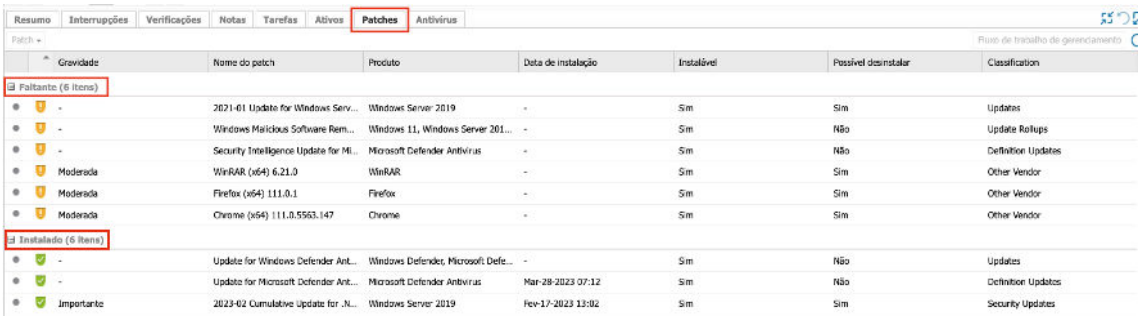
4. Ativação e Políticas

É possível realizar a ativação do **Gerenciamento de Patches** de duas formas: massiva e unitária.

Por **este link** do manual do **N-sight RMM** explicamos como fazer a ativação do recurso, das duas formas.

Assim que o **Gerenciamento de Patches** for ativado no dispositivo, ele automaticamente executará uma varredura em busca pelos status dos patches, trazendo em uma verificação (na aba Verificações) quais são os patches faltantes do dispositivo (tanto Microsoft como de terceiros).

Então na guia **Patches**, para o dispositivo, serão exibidos o status de instalação atual, juntamente com a gravidade do patch, o nome do patch, o produto, data da instalação, se permitem ser desinstalados e a classificação do patch, determinado pelo fabricante.

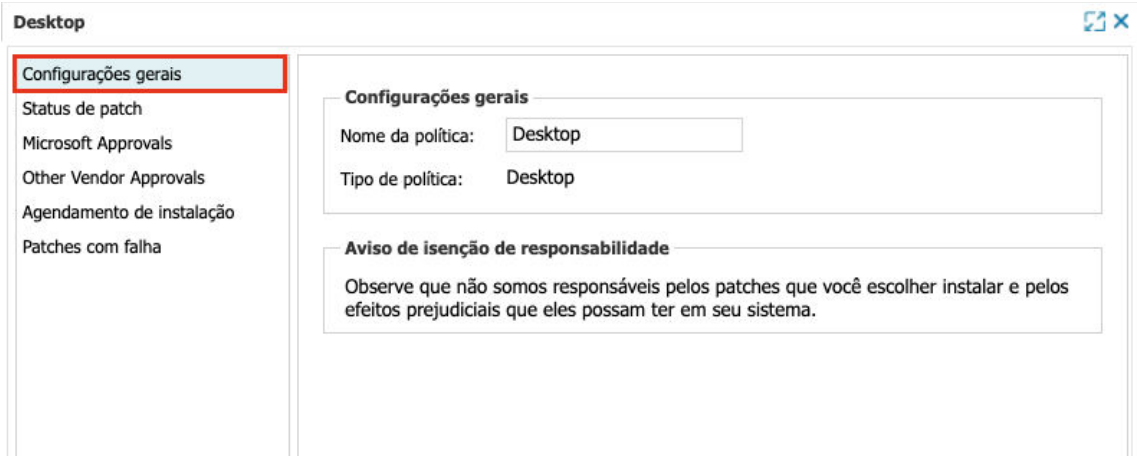


As políticas controlam cada aspecto do Gerenciamento de Patches, desde o tipo de proteção oferecida, incluindo o agendamento de verificações, ação de remediação e o comportamento do alerta.

Abaixo temos algumas informações básicas sobre a configuração da política, mas você pode analisar as informações com mais detalhes acessando **este link** do manual da solução.

+ Configurações Gerais

Podemos alterar o “Nome da Política” e exibir os tipos de dispositivos aos quais esta política pode ser utilizada, além do aviso de isenção de responsabilidade pela instalação dos patches nos dispositivos.

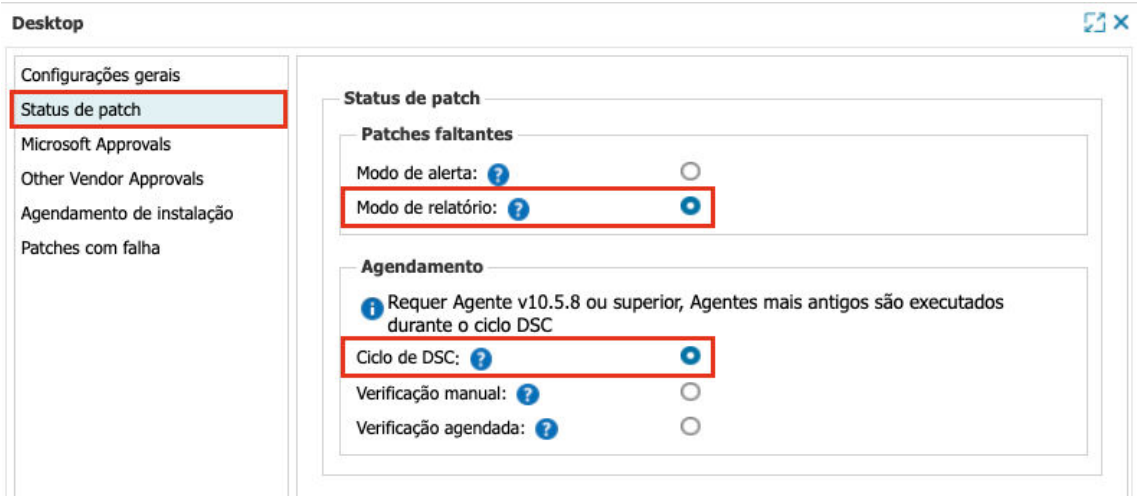


+ Status de Patch

Podemos configurar quando será feita a busca por novos patches no dispositivo local.

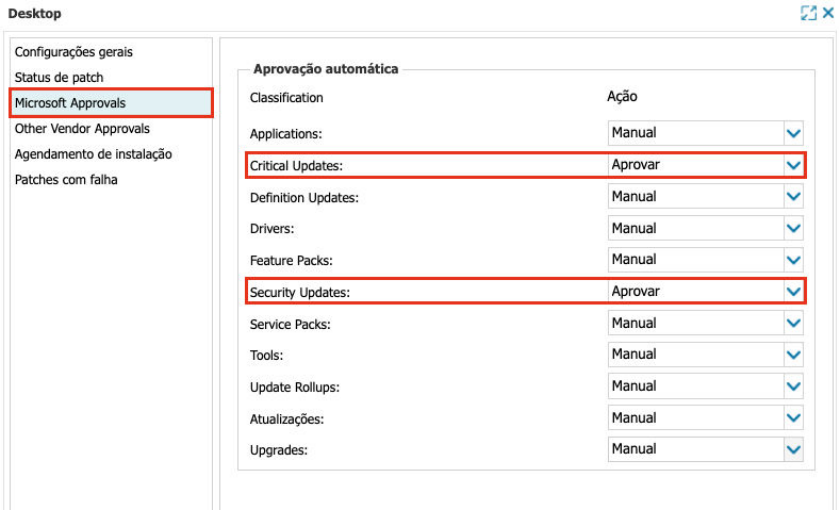
Recomendamos que seja utilizado o “modo relatório” no início de cada implantação até que todo o ambiente esteja atualizado.

Depois, para o agendamento, você pode utilizar a opção “ciclo de DSC”, pois esta busca será realizada todos os dias.



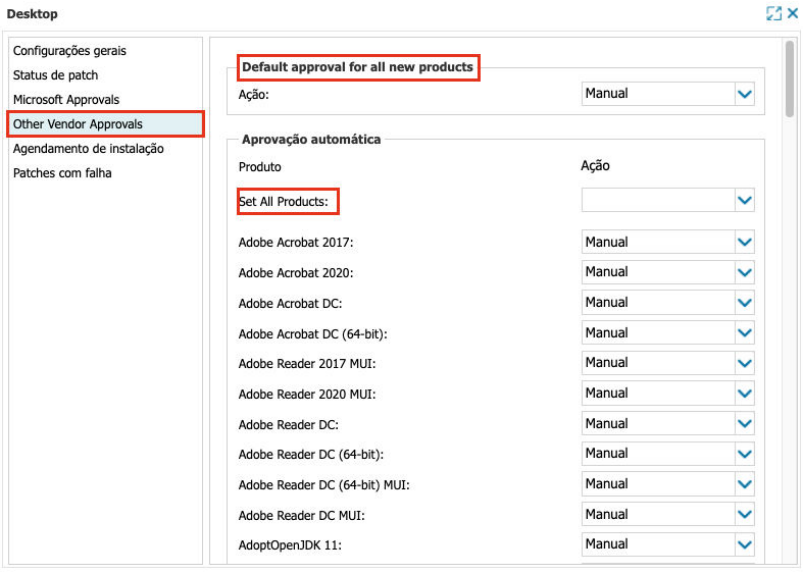
+ Política de Aprovação (Microsoft Approvals)

Podemos definir as regras de aprovação de patches da Microsoft antes da implantação dos patches, com base em sua classificação. Recomendamos a configuração de aprovações automáticas pelo menos para os patches de classificação críticas (**Critical Updates e Security Updates**).



+ Política de Aprovação (Other Vendor Approvals)

Podemos definir as regras de aprovação para patches de terceiros antes da implantação dos patches com base em sua classificação. Veja que há a possibilidade de deixar como padrão a aprovação automática para novos produtos adicionados nesta lista (não recomendado), e também a opção de “setar” a automação para todos os produtos da lista de uma só vez.

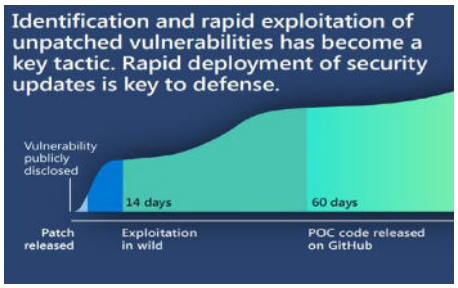


+ Considerações de segurança ao gerenciar patches

A **Microsoft** observou que leva apenas 14 dias, em média, para que uma exploração esteja disponível após a divulgação pública de uma falha, afirmando que, embora os ataques de dia zero sejam inicialmente limitados em escopo, eles tendem a ser rapidamente adotados por outros atores de ameaças, levando a eventos de investigação indiscriminados antes da instalação dos patches.

Devido a isso, é altamente recomendável que você adote uma estratégia de aprovar/ignorar patches semanalmente, em vez de mensalmente.

Isso garante que a maioria dos dispositivos permanecerá atualizada com os patches de segurança recentes e você também reduzirá a superfície de ataque dos dispositivos internos ou clientes sob gerenciamento.



FONTE: https://www.microsoft.com/en-us/security/business/ microsoft-digital-defense-report-2022

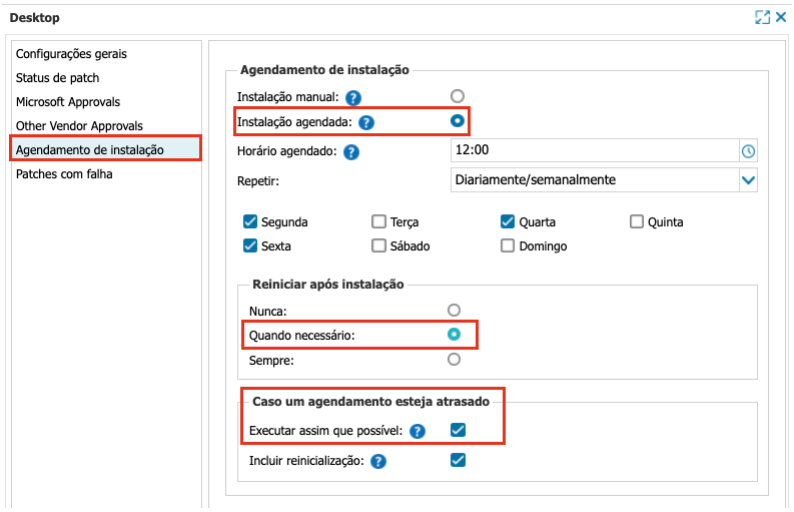
+ Agendamento da Instalação

Aqui podemos definir quando os patches aprovados anteriormente serão instalados nos dispositivos.

Recomendamos que a instalação seja feita de forma agendada para estações de trabalho, de preferência fora do horário comercial ou do horário de expediente do cliente, e configurar para reiniciar os dispositivos apenas quando necessário.

Para servidores, recomendamos a instalação manual e acompanhada.

A opção **“Executar assim que possivel”**, na seção **“Caso um agendamento esteja atrasado”**, é muito importante mantê-la ativada, pois em casos onde uma atualização crítica foi lançada e haviam muitos dispositivos offline durante a janela de instalação, assim que estes dispositivos ficarem online a instalação do patch será realizada no ato, não sendo necessário aguardar a próxima janela de instalação.



Apenas fique atento se a política de instalação inclui a reinicialização do dispositivo, para evitar que o dispositivo seja reiniciado em um momento inoportuno.

+ Patches com Falha

Caso o agente não consiga instalar o patch no dispositivo (seja porque o mesmo foi desligado no momento da instalação ou talvez porque o dispositivo estava com muito processamento em uso naquele momento), podemos configurar algumas ações automáticas para o painel realizar, como reprocessar a instalação até 5 vezes, e encaminhar um e-mail em caso de nova falha.

Nossa recomendação é reprocessar a instalação em no máximo 2 vezes, levando em consideração a política de instalação.

Também não deixe de acompanhar o Relatório de Patches com Falhas para ficar por dentro de todos os patches que falharam na instalação.

5. Fluxo de Trabalho de Gerenciamento

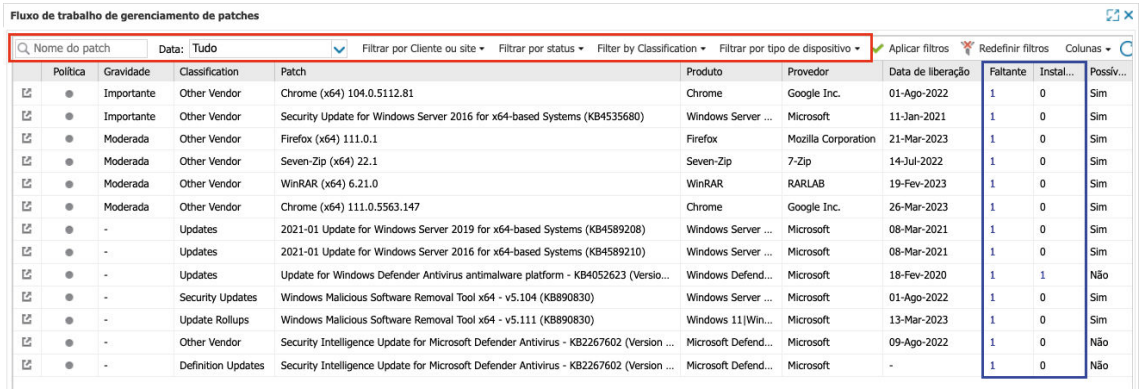
O **N-sight RMM** oferece, além da possibilidade de você poder administrar todos patches e atualizações dos dispositivos de forma individual, sem precisar ter acesso ao dispositivo local, a possibilidade de você ter acesso global de todas as atualizações, de todos os dispositivos do teu painel, não importa o cliente ou o site.

Este recurso se chama **Fluxo de Trabalho de Gerenciamento**, e através dele é possível filtrar várias condições de patches (faltantes, instalados, aprovados, etc.) de vários clientes ou dispositivos de uma só vez.

Isto é incrível porque você pode com poucos cliques verificar todos os patches faltantes, ou certificar-se de que todos os patches foram instalados corretamente, tudo em uma única tela.

E o mais interessante é que pelo próprio **Fluxo de Trabalho de Gerenciamento** você pode aprovar ou instalar os patches de forma massiva, independente do dispositivo, site ou cliente.

Basta selecionar o patch a ser instalado e clicar no botão **"Continuar"**. O sistema irá perguntar se você quer aprovar ou ignorar a instalação do patch, vai perguntar para quais clientes você quer aplicar o patch (ou quais tipos de dispositivos: estação ou servidores), e por último vai perguntar quando será realizada a instalação (no ato ou através do agendamento).

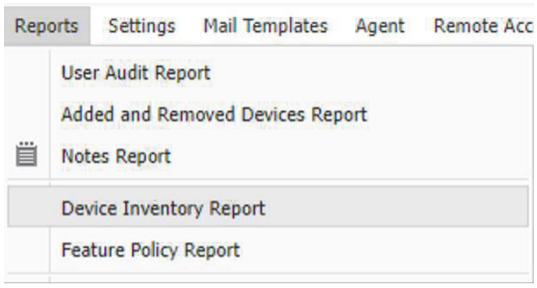


Política	Gravidade	Classification	Patch	Produto	Provedor	Data de liberação	Faltante	Instal...	Possív...
●	Importante	Other Vendor	Chrome (x64) 104.0.5112.81	Chrome	Google Inc.	01-Ago-2022	1	0	Sim
●	Importante	Other Vendor	Security Update for Windows Server 2016 for x64-based Systems (KB4535680)	Windows Server ...	Microsoft	11-Jan-2021	1	0	Sim
●	Moderada	Other Vendor	Firefox (x64) 111.0.1	Firefox	Mozilla Corporation	21-Mar-2023	1	0	Sim
●	Moderada	Other Vendor	Seven-Zip (x64) 22.1	Seven-Zip	7-Zip	14-Jul-2022	1	0	Sim
●	Moderada	Other Vendor	WinRAR (x64) 6.21.0	WinRAR	RARLAB	19-Fev-2023	1	0	Sim
●	Moderada	Other Vendor	Chrome (x64) 111.0.5563.147	Chrome	Google Inc.	26-Mar-2023	1	0	Sim
●	-	Updates	2021-01 Update for Windows Server 2019 for x64-based Systems (KB4589208)	Windows Server ...	Microsoft	08-Mar-2021	1	0	Sim
●	-	Updates	2021-01 Update for Windows Server 2016 for x64-based Systems (KB4589210)	Windows Server ...	Microsoft	08-Mar-2021	1	0	Sim
●	-	Updates	Update for Windows Defender Antivirus antimalware platform - KB4052623 (Versio...	Windows Defend...	Microsoft	18-Fev-2020	1	1	Não
●	-	Security Updates	Windows Malicious Software Removal Tool x64 - v5.104 (KB890830)	Windows Server ...	Microsoft	01-Ago-2022	1	0	Sim
●	-	Update Rollups	Windows Malicious Software Removal Tool x64 - v5.111 (KB890830)	Windows 11|Win...	Microsoft	13-Mar-2023	1	0	Sim
●	-	Other Vendor	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version ...	Microsoft Defend...	Microsoft	09-Ago-2022	1	0	Não
●	-	Definition Updates	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version ...	Microsoft Defend...	Microsoft	-	1	0	Não

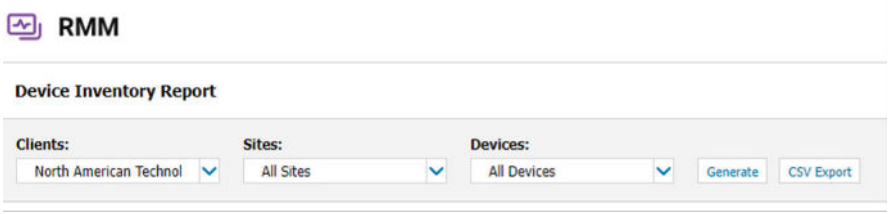
Para acessar o **Fluxo de Trabalho de Gerenciamento** vá em:
Configurações / Gerenciamento de Patches / Fluxo de Trabalho de Gerenciamento.

+ Inventário de Dispositivos

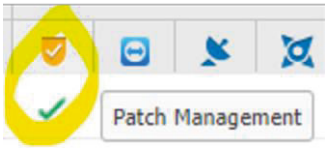
Você pode usar o **Relatório de Inventário** de Dispositivos para confirmar quantos dispositivos não têm o **Gerenciamento de Patches** ativado.



Selecione o **"Cliente"** e clique no botão **"Gerar"**:

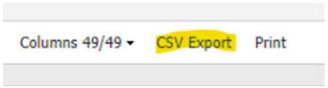


Verifique no lado direito da tabela de dispositivos os recursos habilitados e o ícone **Gerenciamento de Patches**:



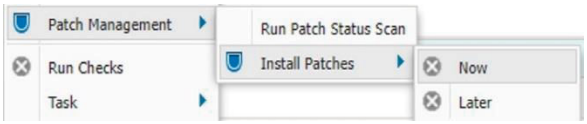
No meu exemplo, tenho todos os dispositivos com o **Gerenciamento de Patches** habilitado, o que me dará uma cobertura total de 100% para este mês.

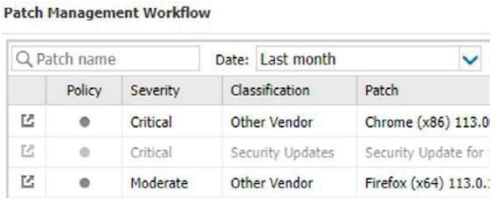
No entanto, você pode não ter todos os dispositivos com o recurso habilitado, então não se esqueça de usar a **exportação CSV** para filtrar facilmente os dispositivos com patch habilitado e obter uma contagem exata.



+ Atividades Diárias

Para aumentar nossa **“Pontuação de Integridade do Patch”**, podemos realizar atividades diárias na aba Patches de cada dispositivo ou usar o **Fluxo de Trabalho de Gerenciamento** para cuidar de mais patches ao mesmo tempo e de mais dispositivos, dependendo dos requisitos.

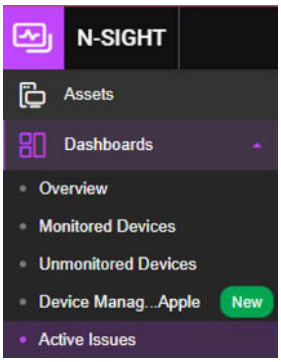


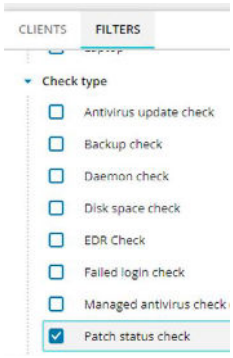


Por mais importante que seja aprovar e ignorar patches, garantir que os patches estejam funcionando conforme o esperado é uma grande parte do nosso serviço de monitoramento de verificação de status de patches.

Você terá cada dispositivo com o recurso habilitado executando este serviço. Isso permite alertar se houver problemas relacionados à comunicação com o Windows Update ou quaisquer instalações pendentes necessárias (se você tiver o status da política de **Gerenciamento de Patches** definido como “Modo de Alerta” para patches pendentes).

Se houver algum problema contínuo e você tiver muitos dispositivos para cuidar, é mais simples usar o painel de **Problemas Ativos**. Verifique em **“Filtros”** a verificação do status do patch:





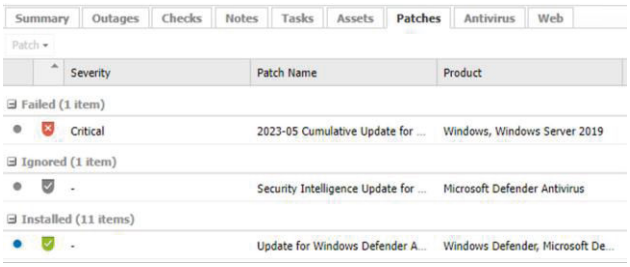
Agora podemos verificar facilmente quais dispositivos estão nos alertando e avaliar rapidamente como corrigir esses problemas.

+ Central de Suporte e Procurando por códigos de erro

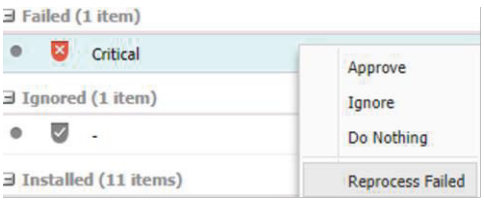
No meu exemplo anterior, tenho um dispositivo relatando uma falha na verificação, então meu próximo passo é ir para a **Central de Suporte da ADDEE** e digitar, por exemplo, “Patch Scan failed” na função de pesquisa.

Também pode haver momentos em que a instalação de um patch falha, seja devido a um pré-requisito que não foi atendido ou a um erro específico relacionado ao próprio patch.

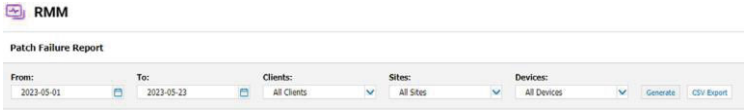
O agente do **N-sight RMM** pode coletar códigos de erro e erros de execução, para que possamos agir mais rapidamente para mitigar tais ocorrências. Podemos ir para a guia **“Patches”** desse dispositivo ou usar o **“Relatório de Falhas”** no **Gerenciamento de Patches**.



A partir daqui também podemos tentar reprocessar diretamente o patch com falha:



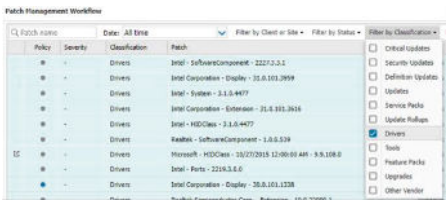
O **Relatório de Falhas**, no entanto, nos dará uma boa visão geral de todos os problemas encontrados.



+ Ignorando Patches

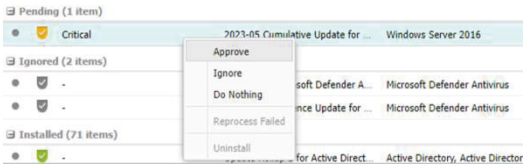
gnorar classificações ou patches específicos é necessário para manter uma pontuação alta de **"Pontuação de Integridade do Patch"**. Qualquer patch detectado e não instalado ou tratado dessa forma afetará significativamente sua pontuação.

Como prática recomendada, vemos parceiros ignorando classificações específicas, como drivers, que normalmente podem ser encontradas por meio do **Windows Update**, mas que exigem intervenção manual.

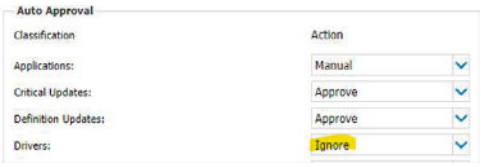


Na imagem acima selecionei **"Todo o Tempo"** em **Datta** e **"Drivers"** em **Classificação**. Assim, posso selecionar facilmente mais de um patch e ignorá-los:

Da mesma forma, você quer ter certeza de que todos os patches que devem ser instalados sejam aprovados, seja em massa ou especificamente em cada dispositivo/patch. Abaixo há um exemplo de patch crítico que requer minha aprovação. Posso clicar com o botão direito na guia **Patches** do dispositivo e clicar no botão **Aprovar** e, em seguida, selecionar se desejo instalar seguindo uma programação anterior, uma nova ou apenas agora.



Na Política de Gerenciamento de Patches, também podemos definir o status de aprovação para classificações específicas, como drivers, como no exemplo acima. A partir deste ponto, todas as atualizações de Drivers descobertas serão automaticamente ignoradas, não afetando a **Pontuação de Integridade** no **Relatório Executivo Resumido**.

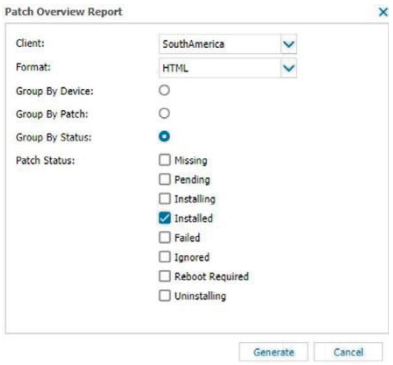


6. Relatórios

Conforme informado anteriormente, os relatórios são cruciais na gestão dos patches, e são sua principal fonte de análise sobre o andamento de suas instalações.

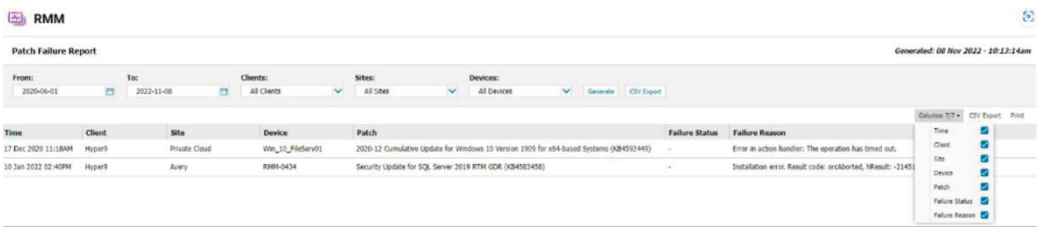
+ Relatório de Visão Geral de Patches

O **Relatório de Visão Geral** fornece detalhes sobre nomes, instalação e status de descoberta de todos os dispositivos com o recurso habilitado. Essas informações podem ser agrupadas por **Dispositivo, Patch** ou **Status** e podem ser exportadas via **HTML**, **CSV** ou **XML** para posterior manipulação.



+ Relatório de Falhas de Patches

O **Relatório de Falhas** ajuda a identificar patches problemáticos, rastreando todas as falhas mesmo que um patch tenha sido concluído. Este relatório nos fornecerá o dispositivo, a hora, o nome do patch e o status da falha junto com o motivo da falha original.



+ Pontuação de Integridade do Gerenciamento de Patches

A Pontuação de Integridade do Gerenciamento de Patches, no Relatório Executivo Resumido, é composta por duas métricas principais: **Cobertura** e **Proteção**.

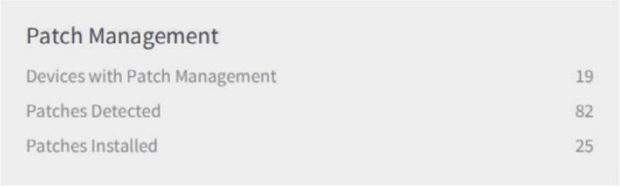
Cobertura

Cobertura é o número total de dispositivos com gerenciamento de patches habilitado em um determinado mês.

Se você tiver 9 estações de trabalho e 1 servidor em um cliente, e apenas o servidor tiver o **Gerenciamento de Patches** habilitado, a cobertura total seria de 10%. No caso acima, todos os dispositivos possuem o **Gerenciamento De Patches** habilitado, portanto, podemos ver 100% de Cobertura.

Proteção

A **Proteção** é um cálculo (divisão) do número total de patches instalados com o número total de patches detectados (este número não inclui patches ignorados, que é um aspecto fundamental dos seus fluxos de trabalho de patches, pois todos os patches que não devem ser gerenciado geralmente deve ser ignorado para aumentar a porcentagem de proteção).



Na figura acima, podemos ver 82 Patches Detectados versus 25 Instalados. Isto dá uma % final de 30,48 de Proteção que é arredondada para a próxima casa decimal para 30,5% (como visto na Figura 4).

Este cliente, de fato, teve 90 patches detectados, mas 8 deles foram marcados como ignorados, portanto, não fizeram parte do cálculo.

Nota
Os totais podem diferir do Dashboard e do Relatório de Visão Geral dos Patches porque a detecção e a instalação dos patches podem abranger vários meses, não apenas o mês especificado em um Relatório Executivo Resumido

7. Detecção de Patches e Como Funciona o PME

+ Validando por que um patch específico não está disponível

Existem algumas situações em que um patch específico que você está procurando não aparece como detectado. É importante entender como o **PME (Patch Management Engine, ou Mecanismo do Gerenciamento de Patches)** funciona para que você tenha uma melhor compreensão de como ele ajuda você e o que procurar ao solucionar problemas.

O mecanismo PME fará uma pesquisa em vários repositórios, incluindo **Windows** e **Microsoft Update, Registro e WSUS e Patch Scanner de terceiros (N- able)**. Se um patch não estiver aparecendo como disponível, pode ser devido a um resultado de verificação desatualizado (certifique-se de verificar se a detecção está definida como automática e diária na Política de Patches e, se necessário, você pode forçar uma verificação em tempo real, acessando o menu de contexto do botão direito do dispositivo) ou um patch que substituiu aquele que você está procurando.

+ O que é Substituição de Patches?

Este é um conceito de **Gerenciamento de Patches** onde um patch desatualizado ou mais antigo e todo o seu conteúdo são totalmente incluídos em um patch lançado posteriormente, mais recentemente. Com isso, se você instalar o patch mais recente, também instalará qualquer conteúdo do patch mais antigo que esteja faltando no dispositivo.

Resumidamente, o **mecanismo PME** fará a varredura do dispositivo e se os resultados da varredura contiverem um patch que substituiu os outros, manteremos apenas este patch mais recente e não mostraremos os mais antigos.

Esta é uma grande vantagem, pois qualquer fornecedor provavelmente recomendará que você instale o patch mais recente que substituiu qualquer outro, pois incluirá mais conteúdo que eles consideram importante corrigir em seus dispositivos. Isso evita que você aprove um patch que pode não ser o mais recente e que não incluiria algumas correções ou complementos do fornecedor.

Em caso de dúvida, verifique novamente no **Catálogo da Microsoft**:
https://www.catalog.update.microsoft.com/

8. Problemas e Erros

As causas dos problemas e/ou erros encontrados podem variar, e cada um requer um procedimento específico para correção. Entretanto, iremos listar abaixo alguns que já foram levantados e solucionados:

+ Erro “Patch Status Scan Not Uploaded”

Este erro **“Patch Status Scan Not Uploaded”** ocorre quando o painel não consegue se comunicar com o serviço do Windows Update do dispositivo.

Neste caso você pode verificar se a comunicação com a internet e o serviço do Windows Update estão OK no dispositivo para ter certeza de que a comunicação entre o dispositivo e os nossos servidores estão ocorrendo normalmente.

Caso esteja tudo ok, tente primeiramente reiniciar o serviço do Windows Update. s vezes ele pode aparentar estar ativo, mas a comunicação dele com o **N- sight RMM** pode ter se perdido.

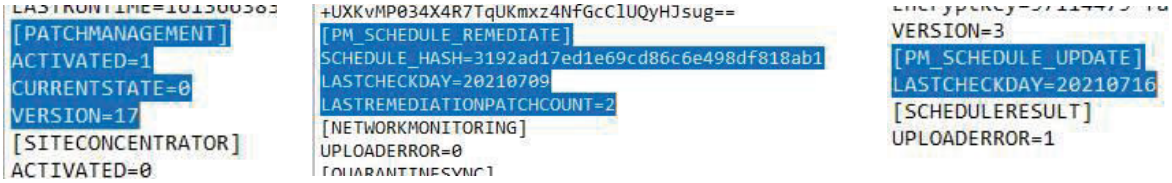
Se nenhum procedimento acima resolver, tente reinstalar o recurso do **Gerenciamento de Patches** para forçar a comunicação novamente, usando o passo-a-passo abaixo:

1. Desative o Gerenciamento de Patches no dispositivo:
    1.1 - No painel RMM, dê um duplo clique no dispositivo para abrir a edição.
    1.2 - Selecione a aba **Gerenciamento de patch** do lado esquerdo.
    1.3 - Altere o campo **Configuração** para **Desligado**.
    1.4 - Clique em **OK** para validar as alterações.
    1.5 - Aguarde até que a desinstalação seja finalizada.

2 - Localmente no device vá na pasta **C:\Program Files (x86)\Advanced Monitoring Agent**.

3 - Edite o arquivo **settings.ini** e apague as entradas:

[PATCHMANAGEMENT], [PM_SCHEDULE_REMEDIATE] e [PM_SCHEDULE_UPDATE]. Apague a chave e todo o conteúdo abaixo dela, até a próxima chave, semelhante ao print abaixo:



4 - Reinicie o dispositivo **(recomendado)**.

5 - Ative o Gerenciamento de patch novamente:
    5.1 - No painel RMM, dê um duplo clique no dispositivo para abrir a edição.
    5.2 - Selecione a aba **Gerenciamento de patch** do lado esquerdo.
    5.3 - Altere o campo **Configuração** para **Ligado** (ou usar Pai).
    5.4 - Clique em **OK** para validar as alterações.
    5.5 - Aguarde até que a instalação esteja concluída.

6 - Após a instalação o recurso irá iniciar um longo processo de busca dos patches, em seguida a verificação deve ser normalizada.

+ Erro “Verificação de Status de Patches”

Para corrigir este erro tente forçar manualmente a execução desta verificação.

Basta clicar com o botão direito sobre o dispositivo, escolher a opção **Gerenciamento de Patches** e selecionar a opção Executar Verificação de Status de Patches.

Aguarde um tempo para que a busca por novos patches seja realizada (este tempo pode variar dependendo do dispositivo/rede).

Caso a opção de forçar a verificação não funcione ou não esteja disponível, é possível que o **Gerenciamento de Patches** esteja corrompido, e somente uma reinstalação do recurso poderá resolver.

Você pode optar por apenas desativar o recurso no painel, aguardar alguns instantes até que o painel informe que o recurso foi desativado, e ativá-lo novamente, como também pode utilizar o procedimento de reinstalação limpa passado na correção do erro anterior.

9. Q & A

+ Já que o GP não lista as atualizações opcionais (tipo “C” e “D”) como posso realizar estas atualizações?

Estas atualizações opcionais podem ser feitas manualmente através do Windows Update do Sistema Operacional.

Mas tenha em mente que a própria Microsoft considera estas atualizações como versões de “preview releases”. Portanto, não foram amplamente testadas, podendo ocasionar algum impacto em seu ambiente.

+ O Gerenciamento de Patches está disponível para dispositivos MacOs?

Embora o produto Gerenciamento de Patches não esteja disponível para dispositivos Mac, há uma tarefa automatizada que instalará patches nos dispositivos Mac, chamada **“Managed Patch”.**

A N-able disponibilizou **este link** do manual que explica como funciona esta tarefa para MacOs.

ADDEE

Empresa brasileira, iniciamos nossas operações em 2013 com o objetivo de revolucionar o mercado de Prestação de Serviços de TI e contribuir com o enriquecimento moral, intelectual e financeiro de nossos clientes e colaboradores.

Nascemos da necessidade de um Prestador de Serviços de TI e hoje somos Distribuidores das melhores ferramentas para Prestadores de Serviços de TI de todo o Brasil.

Trabalhamos para o crescimento sustentável do mercado de tecnologia, através do compartilhamento de conhecimentos e a distribuição de soluções inovadoras para Gestão de TI. Com estrutura local, fornecemos atendimento e suporte em português, além de todo o apoio comercial necessário para empresas de Serviços de TI.

Compreendemos as necessidades locais e por isso somos o principal parceiro de negócios dos nossos clientes.

Com um time de profissionais altamente qualificados e apaixonados por tecnologia e relacionamento, colocamos acima de tudo, as pessoas. É assim que fazemos negócios.

Última alteração: Novembro/2023

Responsável: Caio Gutierri

E-mail: boaspraticas@addee.com.br

YouTube Instagram Linkedin Site Blog