Redes LAN; Aplicação do Active Directory, PfSense, Zabbix e RADIUS para redes de computadores

ÁLVARO REGO LIMA
JOÃO PEDRO MELO COELHO
MATEUS CARNEIRO LIMA
RYAN DOS SANTOS NEVES
MILSON LOUSEIRO LIMA
JORGE HELENO BALDEZ JUNIOR
EWERTON FERREIRA BASTOS

Faculdade Laboro

RESUMO

AO artigo em questão descreve as ferramentas Active Directory, pfSense, o,Zabbix e o RADIUS apresentadas no trabalho avaliativo da segunda nota domprofessor Ewerton no segundo período do ano de 2022. Primeiramente, é apresentada uma visão geral do Active Directory, que é utilizado como o diretório de usuários centralizado da rede. Em seguida, é descrito os conceitos de pfSense, um firewall de código aberto. Além disso, é explicado uma definição de o que é Zabbix, um software de monitoramento de rede, para monitorar o tráfego de rede e coletar informações sobre os usuários que estão acessando a rede. Por fim, é apresentado a idealização de RADIUS, um protocolo de autenticação e autorização, para permitir que usuários autenticados no Active Directory possam se conectar à rede de forma segura e controlada. No geral, o artigo mostra como utilizar essas ferramentas em conjunto para criar uma solução completa de autenticação e controle de acesso em uma rede de computadores.

Palavras chaves: : Active Directory, PfSense, Zabbix, RADIUS.

ABSTRACT

The article in question describes the tools Active Directory, pfSense, Zabbix and RADIUS presented in Professor Ewerton's second grade assessment paper in the second term of the year 2022. First, an overview is presented of Active Directory, which is used as the network's centralized user directory. Next, the concepts of pfSense, an open source firewall, are described. Also, a definition of what Zabbix, a network monitoring software, is, is explained to monitor network traffic and collect information about the users that are accessing the network. Finally, the conception of RADIUS, an authentication and

authorization protocol, is presented to allow users authenticated in Active Directory to connect to the network in a secure and controlled way.

Overall, the article shows how to use these tools together to create a complete authentication and access control solution on a computer network.

Keywords: Active Directory, PfSense, Zabbix, RADIUS

PROTOCOLOS DE GERENCIAMENTO

A evolução do parque eletrônico das empresas torna cada vez mais desafiador a manutenção dos serviços disponíveis nas redes em geral que precisam de estruturas que permitam um gerenciamento amplo e transparente de recursos com a finalidade de

INTRODUÇÃO

Nos últimos anos, a tecnologia tem sido uma grande aliada na gestão e controle de redes de computadores. Entre as soluções mais utilizadas para gerenciar e monitorar essas redes estão o Active Directory, Zabbix, PfSense e Radius. Cada uma dessas ferramentas tem uma função específica, mas juntas, elas podem proporcionar uma gestão completa e eficiente de uma rede. Neste artigo, vamos explorar o uso dessas quatro soluções em conjunto e os benefícios que elas trazem para a administração de uma rede de computadores.

ACTIVE DIRECTORY

O Active Directory (AD) é um serviço de diretório da Microsoft que fornece recursos de autenticação e gerenciamento de identidade em ambientes Windows. Ele permite que os usuários e computadores sejam gerenciados de forma centralizada em um domínio, facilitando o gerenciamento de contas de usuário, políticas de segurança, grupos e outros recursos de rede. Para Wesley Chai o Active Directory é um componente chave da infraestrutura de TI de muitas empresas, fornecendo serviços de diretório e autenticação centralizados.(CHAI, 2000) A importância do Active Directory reside em sua capacidade de fornecer uma infraestrutura centralizada para gerenciar usuários, grupos e recursos de rede. Com o AD, os administradores de rede podem facilmente adicionar, remover ou modificar usuários, controlar o acesso a recursos compartilhados e implementar políticas de segurança em toda a organização. O Active Directory é construído em torno de uma hierarquia de domínios, onde um domínio é uma unidade lógica de administração e segurança que pode ser gerenciada de forma centralizada. Dentro de um domínio, existem

objetos de diretório, como usuários, grupos e computadores, que podem ser gerenciados e organizados de várias maneiras. "O Active Directory é uma das ferramentas mais importantes para a gestão de identidades e acessos em ambientes empresariais.(PORTAL GSTI, 2020), Além disso, o Active Directory

oferece recursos como políticas de grupo, que permitem definir configurações de segurança e outras configurações para usuários e computadores; serviços de certificado, que permitem a emissão e gerenciamento de certificados digitais; e serviços de federação, que permitem que usuários de diferentes organizações acessem recursos de rede uns dos outros

O Active Directory é especialmente importante em ambientes empresariais, onde há muitos usuários e dispositivos que precisam ser gerenciados de forma eficiente e segura. Ele oferece uma plataforma robusta e escalável para a gestão de identidade e acesso, permitindo que as empresas controlem de forma mais eficaz a segurança de seus sistemas e dados. Ao centralizar a autenticação e a autorização, ele simplifica a administração de contas de usuário, reduz a carga de trabalho dos administradores de TI e ajuda a garantir a conformidade com políticas de segurança. Ele também fornece um ponto central para a implementação de políticas de grupo, o que pode ajudar a manter a consistência nas configurações de segurança e outras configurações em toda a rede. Além disso, o Active Directory pode ser integrado a outros serviços da Microsoft, como o Microsoft Exchange, o Microsoft SharePoint e o Microsoft Teams, o que torna o gerenciamento desses serviços mais fácil e eficiente. Em resumo, o Active Directory é uma ferramenta fundamental para a gestão de identidade e acesso em ambientes empresariais, permitindo que as empresas gerenciem de forma centralizada seus recursos de rede, aplicativos e dados, o que é vital para garantir a segurança e eficiência da rede.

PFSENSE

O pfSense é um software livre e de código aberto que funciona como um firewall de rede de computadores. Ele é baseado em FreeBSD, um sistema operacional Unix-like, e é usado para controlar e gerenciar o tráfego de rede em uma variedade de ambientes, como em empresas, escolas, hospitais, instituições governamentais e em sistemas domésticos. O pfSense é uma plataforma de firewall de código aberto altamente respeitada e bem estabelecida que é conhecida por sua estabilidade, segurança e recursos avançados." (TECHTARGET, 2022)

A função principal do pfSense é proteger a rede contra ataques externos e internos, bem como permitir a comunicação entre os dispositivos da rede. Ele oferece recursos avançados de firewall, como filtragem de pacotes, NAT, balanceamento de carga, redirecionamento de porta, VPN, entre outros. O pfSense também pode ser usado para fornecer acesso à internet para dispositivos da rede, permitindo que os usuários configurem políticas de navegação na web e monitorem o uso da banda larga. Ele oferece suporte a vários tipos de conexões à internet, como DSL, cabo, fibra óptica, satélite, entre outros. Além disso,

o pfSense é altamente configurável e personalizável, permitindo que os administradores de rede definem regras e políticas específicas de acordo com as necessidades de sua rede. Ele também é fácil de usar e possui uma interface gráfica amigável, tornando-o acessível mesmo para usuários com pouca experiência em rede.

Resumindo, o pfSense é um software de firewall de rede poderoso e flexível que oferece recursos avançados de segurança e gerenciamento de rede. Ele é amplamente utilizado em todo o mundo em uma variedade de ambientes e é considerado uma ferramenta fundamental para proteger e gerenciar redes de computadores.

ZABBIX

Zabbix é uma plataforma de monitoramento de rede e de sistemas que é amplamente utilizada em ambientes de TI em todo o mundo. Foi criada em 1998 pelo desenvolvedor Alexei Vladishev e é distribuída sob a licença GPL (General Public License). É capaz de monitorar vários tipos de dispositivos, como servidores, roteadores, switches, firewalls, dispositivos de armazenamento, aplicativos e serviços, além de oferecer suporte a vários protocolos de monitoramento, como SNMP, ICMP, JMX, entre outros.

A plataforma oferece uma ampla gama de recursos, incluindo alertas configuráveis, visualização de dados em tempo real, gráficos e relatórios personalizados, além de suporte a múltiplos usuários e permissões de acesso.

A importância do Zabbix está na sua capacidade de fornecer informações detalhadas sobre a infraestrutura de TI de uma organização, permitindo aos administradores de sistema identificar e corrigir problemas antes que eles afetem os usuários finais. Isso ajuda a garantir que os sistemas e serviços estejam disponíveis e funcionando de maneira eficiente, reduzindo o tempo de inatividade e aumentando a produtividade da equipe de TI.

Além disso, o Zabbix é uma ferramenta de código aberto, o que significa que ela é gratuita e pode ser personalizada e estendida de acordo com as necessidades de uma organização. Isso torna o Zabbix uma escolha popular entre empresas e organizações de todos os tamanhos, desde pequenas empresas até grandes corporações.

O Zabbix é uma plataforma essencial para monitorar a infraestrutura de TI de uma organização. Com seus recursos avançados, capacidade de personalização e suporte a múltiplos dispositivos e protocolos, o Zabbix permite que as equipes de TI identifiquem problemas antes que eles afetem os usuários finais, garantindo que os sistemas e serviços estejam disponíveis e funcionando de maneira eficiente. O Zabbix é uma ferramenta que monitora diversos parâmetros em uma rede, dos ativos e equipamentos de um modo geral. Utiliza um mecanismo flexível de notificação que possibilita configurar e-mails de alarmes para quase todos os eventos, produzindo ferramentas que eram relatórios consistentes e funcionalidades que permitem visualizar informações com ênfase nos dados coletados e armazenados (VLADISHEV, 2008)

RADIUS

O RADIUS (Remote Authentication Dial-In User Service) é um protocolo de rede que permite autenticação, autorização e contabilidade (AAA) de usuários que acessam uma rede remota. Ele é comumente usado em redes de acesso remoto, como redes VPN, redes Wi-Fi e serviços de acesso disco.

O RADIUS funciona como um intermediário entre o dispositivo de rede que está sendo acessado (como um servidor de rede ou um roteador) e o usuário que está tentando acessá-lo. Quando um usuário tenta se conectar a uma rede remota, o dispositivo de acesso (como um ponto de acesso Wi-Fi) envia uma solicitação de autenticação para o servidor RADIUS.

De acordo com o livro *Segurança em Redes – Fundamentos*, escrito pelo engenheiro da computação Alexandre Fernandes de Moraes, são características do serviço Radius:

- Baseia-se no modelo cliente servidor, desta forma um mesmo servidor RADIUS pode ser utilizado para atender vários NAS ou clientes na rede ao mesmo tempo.
- Um servidor RADIUS pode servir de Proxy para a autenticação em outros servidores RADIUS.
- Autorização: existem mais de 50 opções no RADIUS que podem ser utilizadas para criar regras de filtragem NAS ou em outros equipamentos clientes RADIUS, possibilitando desta forma autorizar ou negarmos alguns tipos de acessos de usuários.
- Auditoria e contabilidade: além da autenticação e autorização, o servidor RADIUS permite a contabilidade do acesso do usuário, ou seja, dados sobre a sessão do usuário são armazenados e contabilizados. Quando um usuário inicia uma sessão na rede, essa informação é passada ao servidor RADIUS por um pacote inicial. Quando termina, outro pacote informa que a sessão foi terminada e a quantidade de bytes trocados durante ela.
- Vários equipamentos e dispositivos de rede podem ser clientes RADIUS, como roteadores, servidores, firewalls e switches de rede. (MORAES, 2008, p.65)

O servidor RADIUS verifica as credenciais de autenticação do usuário (como nome de usuário e senha) e, se a autenticação for bem-sucedida, o servidor RADIUS informa o dispositivo de acesso que o usuário está autorizado a acessar a rede. O servidor RADIUS também pode fornecer informações adicionais de autorização, como limites de tempo de conexão e privilégios de acesso.

Além da autenticação e autorização, o RADIUS também é usado para contabilidade. Isso

permite que as organizações rastreiem o uso da rede por usuário, para fins de faturamento ou para fins de segurança. Por exemplo, o RADIUS pode ser usado para registrar informações sobre quem acessou a rede, quando eles acessaram e por quanto tempo. A importância do RADIUS está em sua capacidade de garantir a segurança da rede, controlando o acesso de usuários não autorizados e garantindo que apenas autorizados tenham acesso a recursos de usuários de rede. Ele também fornece uma maneira de rastrear o uso da rede e identificar possíveis violações de segurança. O RADIUS é um padrão aberto compatível e amplamente aceito, o que significa que é com uma ampla variedade de dispositivos e tecnologias de rede.

CONSIDERAÇÃO FINAL

O artigo em questão apresenta quatro conceitos importantes na área de redes de computadores: Active Directory, PfSense, Zabbix e Radius. Cada um desses conceitos desempenha um papel fundamental na gestão e segurança de redes corporativas. O Active Directory é um serviço de diretório desenvolvido pela Microsoft que gerencia a autenticação e autorização de usuários e computadores em uma rede. Ele permite que os administradores definam políticas de segurança e configurem permissões de acesso a recursos, além de simplificar a administração de contas de usuário.

O PfSense, por sua vez, é um firewall de código aberto baseado no sistema operacional FreeBSD. Ele oferece recursos de segurança avançados, como VPN, detecção de intrusão e filtragem de conteúdo. O PfSense é amplamente utilizado em ambientes corporativos devido à sua flexibilidade e facilidade de gerenciamento. O Zabbix é uma ferramenta de monitoramento de redes que permite aos administradores monitorar o desempenho e a disponibilidade de servidores, roteadores, switches e outros dispositivos de rede. Ele fornece alertas em tempo real sobre problemas de desempenho e permite a geração de relatórios detalhados sobre o uso da rede. Por fim, o Radius é um protocolo de autenticação e autorização utilizado para gerenciar o acesso a redes sem fio e outros serviços de rede. Ele permite que os administradores definam políticas de segurança para usuários e dispositivos e monitorem o uso da rede em tempo real. Em resumo, o artigo enfatiza a importância de cada um desses conceitos na gestão e segurança de redes de computadores. Ao usar essas ferramentas em conjunto, os administradores podem garantir a integridade e a disponibilidade dos recursos e manter um alto nível de segurança para os usuários e dispositivos conectados à rede.

REFERÊNCIAS

CHAI, Wesley. TechTarget. "What is Active Directory and How Does it Work?". Disponível em; <<https://www.vmware.com/topics/glossary/content/active-directory>>.

PORTAL GSTI, "Active Directory: o que é e como funciona?",<https://www.gsti.com.br/active-directory-o-que-e-e-como-funciona/>)

TECHTARGET. PfSense, 2022. Disponível em<<https://searchsecurity.techtarget.com/definition/pfSense>>

VLADISHEV, A. Manual Zabbix, vs 1.6, 17 ed. 2008.

MORAES, Alexandre Fernandes de. Segurança em Redes: Fundamentos. 1 ed. São Paulo: Erica, 2010