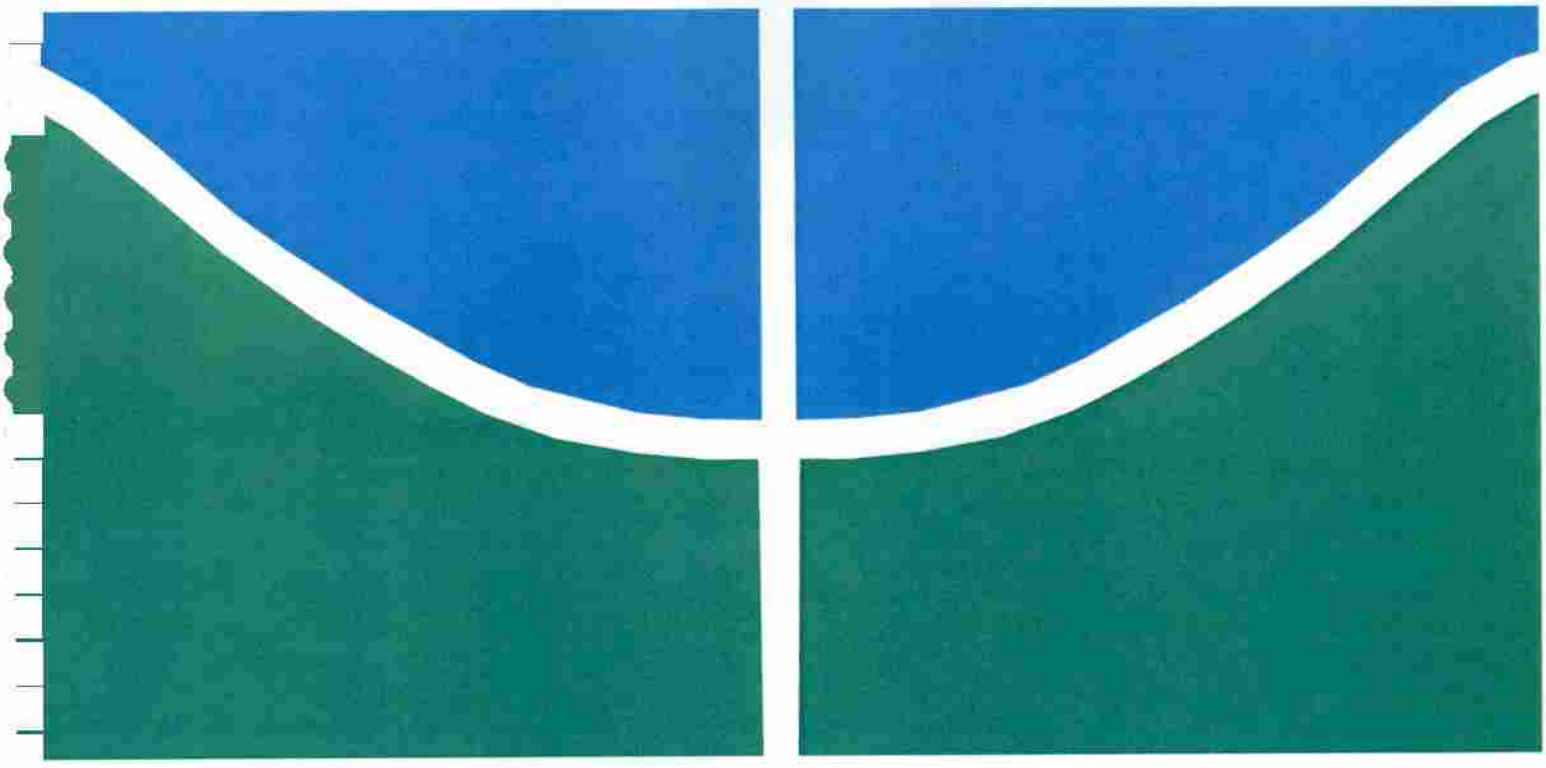


PROPOSIÇÃO DE UM LABORATORIO PARA MONITORAÇÃO E CONTABILIZAÇÃO DE TENTATIVAS DE AUTENTICAÇÃO NO ACTIVE DIRECTORY.

TAIGUARA INDIGENA DO BRASIL

MONOGRAFIA DE CURSO DE ESPECIALIZAÇÃO EM GESTÃO DE SEGURANÇA DA INFORMAÇÃO

DEPARTAMENTO DE ENGENHARIA ELÉTRICA
FACULDADE DE TECNOLOGIA
UNIVERSIDADE DE BRASÍLIA

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

PROPOSIÇÃO DE UM LABORATORIO PARA MONITORAÇÃO E CONTABILIZAÇÃO DE TENTATIVAS DE AUTENTICAÇÃO NO ACTIVE DIRECTORY

TAIGUARA INDIGENA DO BRASIL

ORIENTADOR: ALCYON FERREIRA DE SOUZA JUNIOR

MONOGRAFIA DE CURSO DE ESPECIALIZAÇÃO EM GESTÃO DE SEGURANÇA DA INFORMAÇÃO

BRASÍLIA, DF: AGOSTO / 2017.

UNIVERSIDADE DE BRASÍLIA

FACULDADE DE TECNOLOGIA

DEPARTAMENTO DE ENGENHARIA ELÉTRICA

PROPOSIÇÃO DE UM LABORATORIO PARA MONITORAÇÃO E CONTABILIZAÇÃO DE TENTATIVAS DE AUTENTICAÇÃO NO ACTIVE DIRECTORY

TAIGUARA INDIGENA DO BRASIL

MONOGRAFIA SUBMETIDA AO DEPARTAMENTO DE ENGENHARIA ELÉTRICA DA FACULDADE DE TECNOLOGIA DA UNIVERSIDADE DE BRASÍLIA, COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE ESPECIALISTA EM GESTÃO DE SEGURANÇA DA INFORMAÇÃO.

APROVADO POR:

_____

ALCYON FERREIRA DE SOUZA JUNIOR
MESTRE, UNB/ENE (ORIENTADOR)

_____

CÉSAR AUGUSTO BORGES DE ANDRADE
MESTRE, UNB/ENE (EXAMINADOR INTERNO)

_____

RAFAEL TIMÓTIO DE SOUSA JUNIOR
DOUTOR, UNB/ENE (EXAMINADOR INTERNO)

BRASÍLIA, DF, 31 DE AGOSTO DE 2017.

FICHA CATALOGRÁFICA

Brasil, Taiguara Indígena do.

Proposição de um Laboratório para Monitoração e Contabilização de Tentativas de Autenticação no Active Directory [Distrito Federal], 2017.

Xii, 78p., 210 x 297mm (ENE/FT/UnB, Especialista, Engenharia Elétrica, 2017).

Monografia de Curso de Especialização em Gestão de Segurança da Informação – Universidade de Brasília, Faculdade de Tecnologia.

Departamento de Engenharia Elétrica.

REFERÊNCIA BIBLIOGRÁFICA

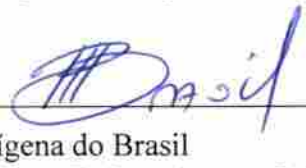
Brasil, Taiguara Indígena. (2017). Proposição de um Laboratório para Monitoração e Contabilização de Tentativas de Autenticação no Active Directory. Monografia, Publicação UnBLabRedes.MFE.050/2017, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 78p.

CESSÃO DE DIREITOS

AUTOR: Taiguara Indígena do Brasil

TITULO DA MONOGRAFIA: Proposição de um Laboratório para Monitoração e Contabilização de Tentativas de Autenticação no Active Directory

GRAU / ANO: Especialista / 2017



Taiguara Indígena do Brasil
SHIGS 707 Bloco B Casa 4 - Asa Sul
CEP: 70.351-702 - Brasília - DF
Tel. 55 – 61 – 98202-1807 / taiguaraindigena@hotmail.com

AGRADECIMENTOS

Gostaria de agradecer especialmente a minha mãe, pelo seu amor incondicional, meus irmãos, irmãs, familiares e todas as pessoas que de alguma forma estiveram em meu convívio, durante esses 39 anos, indiferentemente se em minha analise suas ações foram boas ou ruins, pois todos tem participação no resultado final de formação da minha pessoa, meu muito obrigado a todos.

RESUMO

PREPOSIÇÃO DE UM LABORATORIO PARA MONITORAÇÃO E CONTABILIZAÇÃO DE TENTATIVAS DE AUTENTICAÇÃO NO ACTIVE DIRECTORY

Autor: Taiguara Indígena do Brasil
Orientador: Alcyon Ferreira de Souza Junior
Programa de Pós-graduação em Engenharia Elétrica
Brasília, 31 de Agosto de 2017.

Nas organizações privadas ou públicas, é cada vez maior a busca por controle dos recursos computacionais. Para alcançarmos parte desse controle, utilizaremos a ferramenta de monitoramento Zabbix; para monitorar as tentativas de autenticação em ambientes de domínio Microsoft, através do desenvolvimento de scripts em PowerShell que permitam coletar nos log de segurança do Controlador de Domínio, os registros de tentativas de autenticação realizadas com sucesso ou falha em um determinado período, sendo os scripts acionados pelo agente do Zabbix, implantado no host, seguindo as configurações dos itens relacionados com o host, na ferramenta de monitoramento. A partir de pesquisas bibliográficas e desenvolvimento de um ambiente virtual para a realização de simulações, foram feitas coletas de dados e armazenamento, para posterior análise das informações históricas, que serviram de insumo na construção de linhas de base sobre o funcionamento normal ou não do ambiente e na elaboração de relatórios técnicos, que visam auxiliar as equipes envolvidas na tomada de decisão, dentro das organizações.

ABSTRACT

PREPOSITION OF A LABORATORY FOR MONITORING AND ACCOUNTING FOR AUTHENTICATION TRIALS IN THE ACTIVE DIRECTORY

Author: Taiguara Indígena do Brasil
Supervisor: Alcyon Ferreira de Souza Junior
Programa de Pós-graduação em Engenharia Elétrica
Brasília, 31 August 2017

In private or public organizations, the search for control of computational resources is increasing. In order to achieve part of this control, we will use the Zabbix monitoring tool to monitor authentication attempts in Microsoft domain environments by developing PowerShell scripts that allow us to collect in the Domain Controller security log the authentication logs either successfully or failed over a period of time, with scripts being triggered by the Zabbix agent, deployed on the host, following host-related item settings in the monitoring tool. Based on bibliographical research and the development of a virtual environment for simulations, data and storage were collected for later analysis of historical information, which served as input in the construction of baselines on the normal or non-normal functioning of the environment and in the preparation of technical reports, which aim to assist the teams involved in decision making within organizations.

SUMÁRIO

LISTA DE TABELAS

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE ACRÔNIMOS

AD	*Active Directory*
AMD	*Advanced Micro Devices*
AV	*Ambiente Virtual*
CEO	*Chief Executive Officer*
DDR	*Double Data Rate*
GB	*Gigabyte*
ID	*Identity*
IP	*Internet Protocol*
KDC	*Key Distribution Center*
MHz	Mega-Hertz
MS	*Microsoft*
SCOM	*System Center Operation Manager*
PC	Personal Computer
RFC	*Request for Comments*
SGDB	*Sistema de Gerenciamento de Banco de Dados*
SO	*Sistema Operacional*
SSD	*Solid-State Drive*
VM	Máquina Virtual

1 - INTRODUÇÃO

Com este trabalho estamos buscando desenvolver uma estratégia de monitoramento das tentativas de autenticação de usuários e serviços de rede, realizadas em ambientes compostos por uma infraestrutura de autenticação baseada no Microsoft Active Directory. Também apresentaremos a construção de um ambiente virtual que deverá servir de laboratório para implantação do serviço de autenticação e da infraestrutura de monitoramento, ao qual utilizaremos nas simulações do processo de autenticação e registros em log, para contabilização das autenticações que obtiverem sucesso ou não, no processo. Isso é viabilizado através da construção de scripts em PowerShell que devem ser disparados pela ferramenta de monitoramento e executados através do agente instalado localmente no host monitorado.

No segundo capítulo deste trabalho, abordaremos algumas questões relacionadas ao protocolo Kerberos e o processo de autenticação e auditoria, voltados a infraestruturas baseadas em sistemas operacionais e ferramentas da Microsoft, como os controladores de domínio e o Active Directory.

No terceiro capítulo deste trabalho, abordaremos especificamente a infraestrutura que compõe a ferramenta de monitoramento Zabbix, fornecendo ao leitor as mínimas informações necessárias para a compreensão sobre a ferramenta escolhida para este trabalho, devido a suas características e facilidades de implantação em ambientes computacionais.

1.1 - MOTIVAÇÃO

Apresentar uma opção de ferramenta de monitoramento, que possa coletar e registar o número de tentativas de autenticação realizadas em uma infraestrutura de autenticação baseada no Microsoft Active Directory. Sabemos que no mercado já existem ferramentas com essa característica específica de monitoramento em infraestrutura Microsoft, como é o caso do "Microsoft System Center Operation Manager (MS SCOM)". Mas procuramos por uma ferramenta de monitoramento que permita coletar e armazenar dados dos mais diferentes tipos de equipamentos, Sistemas Operacionais (SO) e aplicações que visa envolver a maior parte possível de uma infraestrutura de redes de computadores, pois sabemos que em sua grande maioria as infraestruturas não são homogêneas. Podendo ter uma infraestrutura de autenticação que mescla o OpenLDAP, Active Directory (AD) e tabelas em banco de dados. A autenticação de usuários e serviços de rede, é o coração da sua infraestrutura de redes de computadores, sendo necessário mantermos um registro histórico simples do volume de tentativas de autenticação que serão realizadas durante um período. Para atender essas necessidades de monitorar vários elementos em sua infraestrutura computacional e especificamente o proposto neste trabalho, optamos por utilizar a ferramenta de monitoramento Zabbix.

1.2 - OBJETIVOS DO TRABALHO

O monitoramento de redes de computadores, existe para automatizar e facilitar o trabalho dos analistas e gestores em uma organização, sendo de suma importância para prevenção e reação a sinais que possam indicar possíveis indisponibilidades de serviços no ambiente. Considerando a autenticação de usuários e serviços de rede um dos pontos centrais dentro da infraestrutura das organizações, queremos explorar através de pesquisas e análises experimentais o monitoramento do número de tentativas de autenticação no Microsoft Active Directory:

a. Apresentar informações sobre o processo de autenticação e auditoria em infraestruturas do Microsoft Active Directory;
b. Apresentar a ferramenta de monitoramento Zabbix e seus principais componentes;
c. Construir um ambiente virtual que permita simulações do processo de autenticação e auditoria;

d. Coletar nos logs do Active Directory o número de tentativas de autenticações executadas com sucesso ou erro;
e. Criar scripts em PowerShell que permitam a contabilização de identificadores (ID) específicos em log, monitorando através do agente Zabbix.

Assim, o principal objetivo deste trabalho é validar uma técnica de monitoramento do número de tentativas de autenticação de usuários e serviços de redes, em uma infraestrutura de autenticação baseada no Microsoft Active Directory, através de resultados coletados em um ambiente de laboratório virtual.

1.3 - METODOLOGIA DE PESQUISA

A metodologia de pesquisa proposta foi dividida em duas etapas para facilitar o entendimento do trabalho, conforme apresentado a seguir:

1° Etapa: Realizar pesquisa bibliográfica, para embasamento teórico sobre os itens que serão abordados no decorrer deste trabalho, sendo utilizados livros, artigos em sites, documentação on-line e revistas;

2° Etapa: Construir um ambiente virtual, que simule uma infraestrutura de autenticação baseada no Microsoft Active Directory, para gerar, coletar e registrar os dados necessários para análise neste trabalho.

1.4 - CONTRIBUIÇÕES DO TRABALHO

Buscam-se com este trabalho as seguintes contribuições:

- Apresentação de uma técnica, para coleta de dados em SO Microsoft, através da chamada de scripts por agente Zabbix;
- Mostrar a importância da construção de linhas de base, que ajudem a identificar possíveis anomalias no ambiente computacional.

1.5 - ORGANIZAÇÃO DO TRABALHO

Para um melhor entendimento deste trabalho, a sua organização é descrita a seguir:

No Capítulo 2; apresentamos algumas considerações sobre autenticação e auditoria, de forma resumida, também tentamos demonstrar de forma didática o processo de autenticação

em ambientes com infraestrutura do Microsoft Active Directory, sendo rapidamente comentado o processo de auditoria em controladores de domínio.

O Capítulo 3; oferece uma revisão literária e compacta das principais características da ferramenta de monitoramento Zabbix, sendo deixado de lado alguns componentes que não serão utilizados neste trabalho.

O Capítulo 4; apresenta a construção e configuração do ambiente virtual, onde serão realizados simulações para geração, registro, coleta, armazenamento, processamento e análise de dados.

O Capítulo 5; conclui este trabalho, apresentando as considerações realizadas sobre os resultados obtidos no laboratório do capítulo 4.

2 AUTENTICAÇÃO

"A autenticação é o processo de determinar se alguma pessoa, ou algo, é realmente quem diz ser." (MORAES, 2010, p. 47). Uma forma mais fácil para assimilarmos essa ideia, é lembrarmos de uma situação corriqueira na vida de um cidadão, onde em algumas vezes precisará autenticar cópias de documentos através de um tabelião de cartório; que executará o processo de autenticação da cópia, dando valor de autenticidade aos dados contidos na cópia do documento. Outra situação cotidiana é quando recebemos uma ligação não identificada (número restrito ou desconhecido), mas somos capazes de identificar e reconhecer (autenticar) a pessoa que está do outro lado da ligação, simplesmente através da voz. Na área de tecnologia da informação e segurança, a autenticação, é um processo primordial para as atividades necessárias ao funcionamento de um ambiente computacional (DIÓGENES & MAUSER, 2013). Em um ambiente computacional precisamos determinar com exatidão a identidade do solicitante; para permitirmos o estabelecimento de um canal de comunicação seguro, que permitirá o tráfego de informações privadas entre as partes, mas esse resultado não é obtido de forma simples, sendo necessário o uso de protocolos com criptografia (TANENBAUM, 2003).

2.1 METODOS DE AUTENTICAÇÃO

Os métodos de autenticação são recorrentemente tratados pelos autores em obras relacionadas a área de segurança da informação e tecnologia. O processo de autenticação na área de tecnologia pode ser fundamentado em um ou mais, dos seguintes métodos:

- "**Com base no que o usuário sabe:** senha, chave criptográfica ou *Personal Identification Number* (PIN)." (NAKAMURA & GEUS, 2007, p. 364);
- "**Com base no que o usuário possui:** *token*, cartão ou *smart* card." (NAKAMURA & GEUS, 2007, p. 364);
- "**Com base nas características do usuário:** biometria (Seção 11.1.3), ou seja, reconhecimento de voz, impressão digital, geometria das mãos, reconhecimento da retina, reconhecimento de íris, reconhecimento digital de assinaturas etc." (NAKAMURA & GEUS, 2007, p. 364).

Você lembra do segundo exemplo de autenticação citado no capítulo 2, onde há o reconhecimento da pessoa em uma ligação não identificada através da voz. Esse é um

exemplo de autenticação baseado nas características do usuário. Já o exemplo referente a autenticação de um documento está baseado no que o usuário possui, no caso, o documento original. Neste trabalho só será utilizado o método que se baseia em algo que o usuário sabe, uma senha pessoal.

2.2 PROTOCOLO KERBEROS

Kerberos é um protocolo de autenticação desenvolvido pelo MIT na década de 80 e que fora baseado no protocolo Needham-Schroeder, sendo a versão 5 do Kerberos descrita na Request for Comments 1510 (RFC) e implementado pela Microsoft em seu SO a partir da sua versão Windows 2000 (TANENBAUM, 2003) e (ZÚQUETE, 2013). O protocolo kerberos possui três componentes principais a sua operação (DIÓGENES & MAUSER, 2013), como descrito a seguir:

O Authentication Server (AS): Atua no processo de validar ou não, a autenticação do solicitante.

O Ticket-Granting Server (TGS): Atua emitindo bilhetes, que serão utilizados pelo solicitante para comprovar sua identidade junto a outros servidores.

Servidor alvo: servidor que possui ou hospeda o serviço solicitado por um cliente.

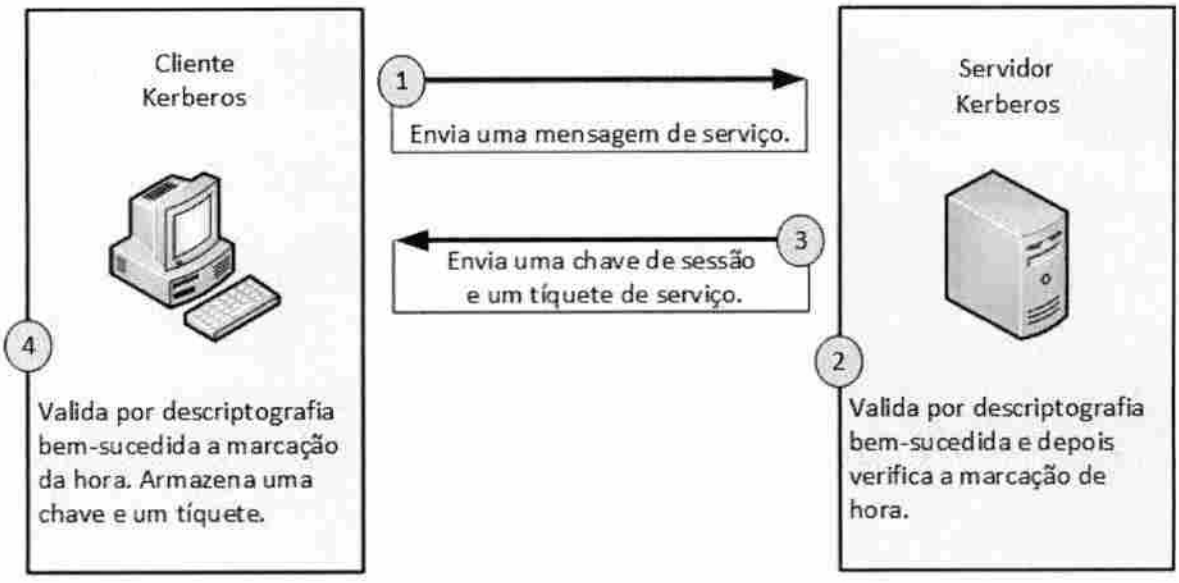
No kerberos, o processo de autenticação acontece através da realização da seguinte interação entre os envolvidos: um cliente envia uma solicitação de acesso a um serviço na rede, ao servidor de autenticação na rede (AS e ou TGS); o servidor responde ao solicitante, com um ticket para o serviço e uma chave de sessão. O solicitante agora utiliza sua chave para descriptografar o conteúdo recebido e utilizar o ticket para provar sua identidade ao servidor, que possui o serviço que o cliente deseja acessar. A chave de sessão é utilizada para estabelecer um canal de comunicação seguro com o servidor alvo. Essa interação permite que o solicitante prove sua identidade aos servidores envolvidos, como também os servidores provem a sua identidade ao cliente.

2.3 PROCESSO DE AUTENTICAÇÃO NO ACTIVE DIRECTORY

Conforme apresentado na seção 2.2, os sistemas da Microsoft tem seu processo de autenticação baseado em uma implantação da versão 5 do protocolo Kerberos. Vamos de forma resumida e simplificada, apresentar os processos envolvidos nessa implantação. Os controladores de domínio em um ambiente de redes com infraestrutura de autenticação do

Microsoft Active Directory, hospedam cópias do banco de dados do domínio, contendo objetos e seus atributos, entre esses atributos temos o nome de usuário e senha, que foram previamente cadastrados; na verdade a senha armazenada é um valor de hash não reversível por padrão, que fora derivado da aplicação de um algoritmo matemático contra a senha do usuário, armazenar o hash em vez da senha, é mais seguro (HOLME, RUEST, RUEST, & NORTHRUP, 2009). Segundo (STALLINGS, 2008, p. 234) "O código de hash é uma função de todos os bits da mensagem e oferece uma capacidade de detecção de erros: uma mudança em qualquer bit ou bits na mensagem resulta em uma mudança no código de hash". Sabendo dessas informações podemos passar para um resumo dos passos utilizados no processo de autenticação; quando um usuário solicita acesso a um recurso de rede, enviando do seu dispositivo (smartfone, notebook, PC) uma solicitação de acesso à rede, contendo em texto claro o nome do domínio, nome do usuário e uma marcação de data e hora, que está codificada por uma chave compartilhada (senha do usuário), quando o KDC (Controlador de Domínio) receber essa solicitação ele busca o nome de usuário na base do AD, caso exista ele recupera a senha armazenada e a utiliza para decriptar os dados, conseguindo, ele verifica se a marcação de data e hora não é inferior a menos 5 minutos, que a hora atual do controlador de domínio, ou seja se o conteúdo codificado for recuperado e estiver dentro do tempo aceito, será considerado como autentico a identidade do solicitante, agora o KDC envia uma chave de sessão ao solicitante, sendo está codificada com a chave compartilhada (senha do usuário), o solicitante então usa sua senha para decriptar a chave de sessão e verifica o carimbo de hora que não deve ser menor que 5 minutos da hora atual do Controlador de Domínio, sendo positivo, o solicitante autentica a identidade do servidor KDC (STANEK, 2009). Sendo que neste trabalho estamos interessados somente na primeira parte do processo, a autenticação do solicitante pelo servidor.

Figura 2.1 - O processo de autenticação do Kerberos.



Fonte: (STANEK, 2009).

Lembramos que o conteúdo apresentado nessa sessão não é completo, e sim resumido, devido a sua extensão, mas você pode obter mais detalhes consultando as literaturas referenciadas durante este trabalho. Destaque para a obra de (STALLINGS, 2008) que detalha mais profundamente o protocolo Kerberos em sua versão 5, que é a utilizada pelo Microsoft Active Directory.

2.4 AUDITORIA

Quando uma solicitação de acesso a rede é recebida por um controlador de domínio do Microsoft Active Directory, ela é processada conforme informado na seção 2.3, e independente do resultado positivo ou negativo da solicitação, o sistema deverá registrar em logs de segurança essa tentativa de autenticação e ou acesso. Permitir no futuro rastrear e determinar quem e quando foram executadas essas tentativas, através de auditorias. Claro que esse registro em log depende da previa configuração do seu Controlador de Domínio, mas isso só será apresentado no capítulo 4, deste trabalho. O registro em log das tentativas de autenticação é primordial para que possamos atingir o objetivo de contabilizar o número de tentativas de autenticação.

Neste capítulo foram apresentados alguns aspectos relacionados ao protocolo Kerberos e o processo de autenticação utilizado pela Microsoft em seus sistemas. Não foram detalhados o protocolo nem sua implantação, por não serem esses o objetivo deste trabalho. Ficamos limitados à parte que autentica o solicitante, informando onde o leitor pode encontrar um conteúdo mais completo, caso sinta necessidade de se aprofundar no conhecimento do protocolo. Também falamos sobre a auditoria que é item importante para atingirmos nosso objetivo final. Já no próximo capítulo iremos apresentar alguns aspectos da ferramenta de monitoramento, que será utilizada neste trabalho.

3 FERRAMENTA DE MONITORAMENTO ZABBIX

Zabbix é um software de código aberto, para monitoramento de infraestruturas de redes de computadores e aplicações, que foi projetado e desenvolvido inicialmente por Alexei Vladishev, e atualmente seu desenvolvimento é mantido pela equipe da Zabbix SIA, empresa que tem como fundador e CEO, o próprio Alexei Vladishev, sendo a fonte de renda desta empresa composta pelas seguintes atividades: Customização, implantação, treinamento, suporte e consultoria na ferramenta de monitoramento Zabbix (ZABBIX SIA, 2017). Esta ferramenta é considerada de nível intermediário em sua implantação e conta com uma comunidade bem ativa que pode fornecer ajuda na resolução de dificuldades, na implantação e customização da ferramenta para o seu ambiente, principalmente se o ambiente for de grande porte (LIMA, 2014). As características de código aberto, modularidade, facilidade de implementação e suporte por muitas comunidades, tornam essa ferramenta de monitoramento adequada aos objetivos deste trabalho.

3.1 PRINCIPAIS COMPONENTES DA FERRAMENTA ZABBIX

A arquitetura da ferramenta de monitoramento Zabbix é composta por vários componentes, sendo que especificamente para atender as necessidades deste trabalho, só pretendemos utilizar alguns que serão descritos nesse capítulo.

3.1.1 Servidor

"O Zabbix Server é o componente centra da solução." (ZABBIX SIA, 2017, p. /concepts/server). Sendo o responsável por receber ou coletar dados através de verificações simples, agentes ou proxy, enviar dados para o armazenamento em banco de dados, utiliza-los na composição e processamento de informações, calcular a necessidade de geração e envio de alertas, conforme regras preestabelecidas pelos administradores (HORST, PIRES, & DÉO, 2015). Neste trabalho o componente servidor será o responsável por coletar e armazenar os dados necessários dentro do nosso ambiente virtual.

3.1.2 Banco de dados

O banco de dados é o responsável por armazenar todos os dados, informações e configurações, repassadas ou geradas pelo servidor ou pela interface web (HORST; PIRES; DÉO, 2015). Podemos definir um banco de dados de uma forma muito simples, como sendo um agrupamento de dados (PLEW; RYAN; STEPHENS, 2003). Este componente, dentro deste trabalho, é responsável pelo armazenamento dos dados, que serão utilizados na construção de gráficos de estatísticas, históricos e linha de base.

3.1.3 Interface Web

A interface web, é meio pelo qual podemos interagir com a ferramenta de monitoramento, visualizando, configurando e gerando relatórios dos mais diversos parâmetros necessários para o monitoramento de sua infraestrutura (HORST; PIRES; DÉO, 2015). Esse componente será o mais utilizado pelas equipes de infraestrutura das organizações, pois é através dele que conseguimos executar configuração, visualização e monitoramento dos itens dentro das organizações e também neste trabalho.

3.1.4 Proxy

Proxy, pode receber ou coletar dados da sua infraestrutura e armazená-los temporariamente em um banco de dados local (buffer), posteriormente repassar esses dados através de rajadas ao servidor Zabbix, dividindo assim a carga gerada sobre o servidor Zabbix (ZABBIX SIA, 2017). Não sendo exigido por esse componente, grandes recursos de hardware e sendo opcional a sua implantação (HORST; PIRES; DÉO, 2015). Mas é altamente recomendado sua aplicação, devido ao fato de possuir banco de dados local, permitindo que o servidor ou o banco de dados do Zabbix possa ficar pequenos períodos indisponível, quando necessária manutenção programada ou não, sendo possível a recuperação dos dados após esse período, junto ao servidor proxy. Esse componente fora citado pela sua importância em ambientes de produção, mas não será utilizado por este trabalho.

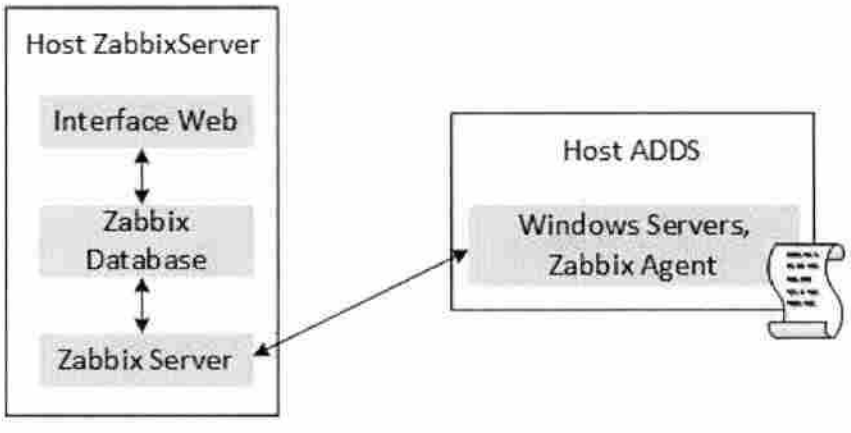
3.1.5 Agente

O agente do Zabbix é um software que pode ser instalado em servidores e estações com SO Microsoft ou Linux, sendo capaz de coletar vários parâmetros do seu hospedeiro e posteriormente repassar ao servidor ou proxy, conforme configurado pelos administradores,

sendo capaz de operar de modo passivo, onde ele executa coleta dos dados de parâmetros locais no hospedeiro mediante a solicitações oriundas do proxy ou do servidor, ou então de modo ativo; busca periodicamente a lista com os itens e períodos de coleta que deve ser executada no hospedeiro, e os armazena localmente, transmitindo rajadas para o proxy ou servidor, conforme previamente configurado (ZABBIX SIA, 2017). Neste modo temos tolerância a falhas no lado do servidor, pois o agente também trabalha com buffer local, permitindo recuperação dos dados (HORST, PIRES, & DÉO, 2015). O agente é basicamente instalado como um serviço no SO do hospedeiro, onde é criado um arquivo contendo diversos parâmetros de suas configurações. Sendo o "UserParameter" o principal parâmetro de interesse desse trabalho, que nos permitirá chamar e executar scripts no host monitorado (HORST, PIRES, & DÉO, 2015). Em nosso trabalho este componente será o responsável por coletar os dados no host, através da chamada de scripts, mediante a solicitações oriundas do servidor Zabbix.

Além dos componentes já informados anteriormente, a ferramenta ainda possui outros componentes que apenas iremos citar seu nome, como o "Java gateway", "Sender" e "Get". Você pode e deve ler o manual do Zabbix, no site da Zabbix SIA, que é o local mais indicado e com maior volume de informações a respeito desta ferramenta. Podemos observar na Figura 3.1 uma representação visual do cenário de monitoramento que pretendemos implantar, neste trabalho.

Figura 3.1 - Cenário de monitoramento pelo Zabbix, neste trabalho.



Fonte: baseado em (HORST, PIRES, & DÉO, 2015).

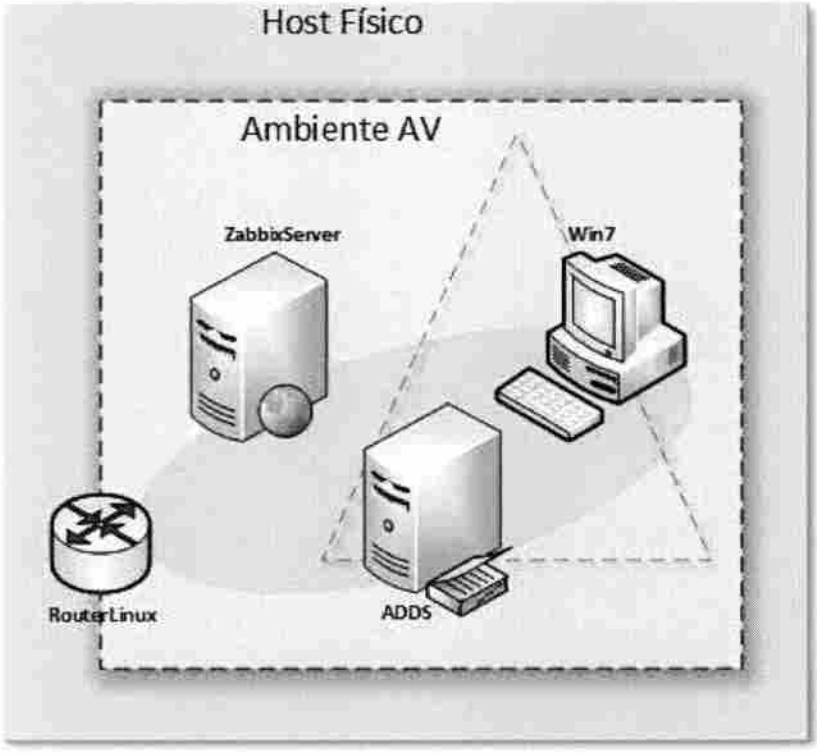
Neste capítulo conseguimos apresentar alguns dos principais componentes da ferramenta de monitoramento Zabbix, descrevendo de forma bastante resumida a função de cada um dos

componentes dentro da infraestrutura de monitoramento e mostrando através da Figura 3.1 qual cenário de implantação pretendemos utilizar neste trabalho. No próximo capítulo iremos tratar da implantação de um laboratório virtual, para simular, coletar, contabilizar e analisar os dados de tentativas de autenticação no Microsoft Active Directory.

4 CONSTRUÇÃO DO AMBIENTE VIRTUAL, SIMULAÇÃO, COLETA E ANÁLISE DE DADOS

Este capítulo trata da construção de um ambiente virtual que será usado como laboratório, afim de possibilitar as simulações necessárias para geração de dados, que serão os insumos utilizados em conjunto com o material teórico, para análise neste trabalho. Os servidores virtualizados são similares aos servidores físicos e ajudam no melhor aproveitamento do hardware, (VERAS, 2011), sabendo dessas características, recursos disponíveis e as atuais facilidades oferecidas pelos Hypervisor que segundo (VERAS, 2011, p. 101) "é a plataforma de máquina virtual". Optamos por essa tecnologia e vamos de agora em diante nos referirmos a este Ambiente Virtual, como simplesmente "AV". Visando tornar mais prático e menos cansativo as diversas citações a este ambiente, que fora pensado para oferecer mobilidade. Na Figura 4.1 temos uma representação visual da infraestrutura do AV.

Figura 4.1 - Representação do Ambiente Virtual (AV).



Fonte: própria.

A infraestrutura do AV é composta por uma rede IP "10.0.0.0/24", com quatro máquinas virtuais (VM's), que segundo (VERAS, 2011) "Uma máquina virtual é um CONTAINER de software totalmente isolado e capaz de executar sistemas operacionais e aplicações próprias como se fosse um servidor físico.". Duas rodando SO Linux e duas VM's rodando SO Microsoft, conforme pode ser visto na Tabela 4.2, sendo que a VM "RouterLinux" desempenha a função de roteamento de pacotes TCP/IP, a VM "ZabbixServer" desempenhará a função de monitoramento, a VM ADDS será encarregada da função de Controlador de Domínio do domínio "abc.interno", a última é de estação de trabalho que será desempenhada pela "VM Win7".

4.1 HYPERVISOR

O Hypervisor escolhido para suportar o AV, conforme informado na Tabela 4.1, fora o Oracle Virtual Box v.5.1 com seu Extension Pack 5.1, que é uma ferramenta de virtualização gratuita e com ampla adoção pelo mercado, será implantado sobre um host físico, com processador AMD FX-8370E com 8 núcleos lógicos, 32GB de memória DDR3 1866Mhz, 480GB SSD, rodando o SO Microsoft Windows 8.1 Profissional, como não existe complexidade na instalação dessa ferramenta em Sistemas Operacionais Microsoft, não apresentaremos os procedimentos, mas você pode encontrar com facilidade na Internet vários sites com tutorias e vídeos, além do próprio site do desenvolvedor https://www.virtualbox.org/ que os ajudaram nesse procedimento, caso não esteja familiarizado com este Hypervisor.

Tabela 4.1 - Software, versão e link para download

Software	Link para download
Oracle VirtualBox 5.1	http://download.virtualbox.org/virtualbox/5.1.22/VirtualBox-5.1.22-115126-Win.exe
VirtualBox Extension Pack 5.1	http://download.virtualbox.org/virtualbox/5.1.22/Oracle_VM_VirtualBox_Extension_Pack-5.1.22-115126.vbox-extpack

Fonte: "https://www.virtualbox.org".

4.2 CRIAÇÃO DAS VM'S

Começaremos criando as VM's em nosso hypervisor, instalando e configurando o SO usando como senha de root ou de Administrador "123456Ab" e seguindo outras informações conforme apresentadas na Tabela 4.2. Não se esqueça também de atualizar o sistema operacional, logo após sua instalação.

Tabela 4.2 - Valores de configuração das VM's

Configure a vCPU para utilizar 75% da CPU, em todas as VM's.					
Hostname	**vCPU**	**vMEM**	**VDI**	**Rede/Gateway**	**SO**
RouterLinux	2	1024 GB	8 GB	10.0.0.250/24 192.168.1.250/24	CentOS 7 "Minimal"
ZabbixServer	2	1024 GB	20 GB	10.0.0.242/24 GW: 10.0.0.250	CentOS 7 "Minimal"
ADDS	2	4096 GB	50 GB	10.0.0.1/24 GW: 10.0.0.250	Windows Server 2012 R2
Win7	2	2048	30 GB	10.0.0.30/24 GW: 10.0.0.250	Windows 7 Profissional

Fonte: própria.

Essas VM's serão utilizadas no nosso AV e darão o suporte necessário aos objetivos deste trabalho, como primeira medida após a instalação, atualização e configuração da VM "ZabbixServer", vamos executar os comandos apresentados no Quadro 4.1:

Quadro 4.1 - Comandos para desativar o SELINUX e reiniciar o servidor

```
# sed –i s/SELINUX=enforcing/SELINUX=disabled/g /etc/selinux/confg
# reboot
```

Fonte: baseado em (HED HAT, s.d.) e (MOTA FILHO, 2012).

Sendo o segundo comando "reboot" necessário para validar as alterações executadas no SElinux, que é uma ferramenta importante na segurança e caso deseje saber mais sobre como configurar essa ferramenta de segurança para trabalhar com o Zabbix, você pode consultar

o capítulo 19 de (HORST, PIRES, & DÉO, 2015). Para atender os objetivos deste trabalho, só desabilitaremos o SElinux.

4.3 CRIAÇÃO DO DOMÍNIO ABC.INTERNO E ATIVAÇÃO DA AUDITORIA DE EVENTOS DE LOGON

Os procedimentos para instalação e configuração do Microsoft Windows Server 2012 r2 são bem intuitivos e para nosso laboratório AV não houve alteração do processo que fora executado sobre a VM ADDS. Conforme informações apresentadas na Tabela 4.2, esses procedimentos podem ser consultados no site da Microsoft ou no capítulo 1 de (ZACKER, 2015). Já a questão dos procedimentos de preparação, implantação e configuração do domínio "abc.interno" do Active Directory, foram executados conforme apresentados no site do Microsoft TechNet (VELTEM, 2014), exceto quando nos fora solicitado informar o nome do domínio e senha, aí fora utilizado os dados da Tabela 4.3, mas você também pode consultar a título de conhecimento o capítulo 5 de (ZACKER, 2015), que trata desse assunto. No mais, recomendamos que você sempre verifique os logs, antes de promover um servidor a controlador de domínio, para assegurar que não haja nenhum erro que deva ser tratado e ou corrigido antes da promoção do servidor.

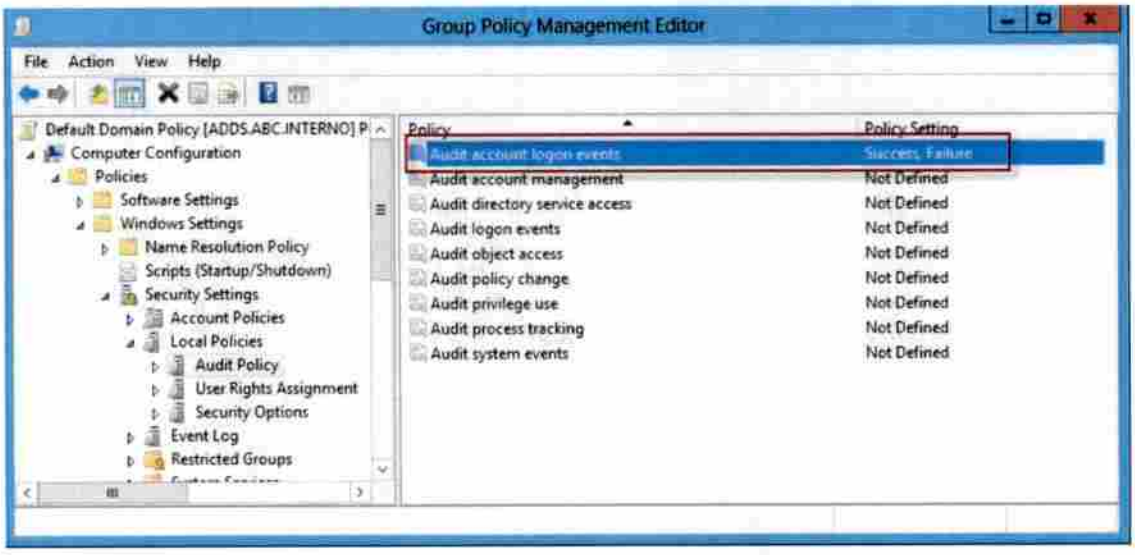
Tabela 4.3 - Dados de conta de usuários do domínio "abc.interno"

Nome de usuário (Username)	Senha (Password)	Perfil
Administrador	123456Ab	Admin/Domain Admins
joao@abc.interno	123456Ab	Domain Admins
maria@abc.interno	123456Ab	Usuário

Fonte: própria.

Depois que terminar de executar os procedimentos relatados anteriormente, vamos configurar a auditoria de evento de logon de conta, para que seja registrado em log no host ADDS as tentativas de logon no domínio. Seguindo as informações relatadas na lição 2 do capítulo 8 de (HOLME, RUEST, RUEST, & NORTHRUP, 2009), foram executadas as configuração necessárias, conforme destacado na Figura 4.2.

Figura 4.2 – Destaque da configuração da auditoria de evento de logon de conta, no domínio "abc.interno".



Fonte: própria.

Agora que já está configurado o registro em log, no controlador de domínio, precisamos de no mínimo uma VM para atuar como estação de trabalho no domínio "abc.interno". Então vamos configurar a VM Win7 para desempenhar essa função, instalando e configurando conforme os dados da Tabela 4.2 e 4.3. Após esse processo, ingresse a mesma como membro do domínio, esse procedimento é executado substituindo as informações de nome do domínio e senha; das apresentadas no artigo de (FELIPE, 2011).

4.4 INSTALAÇÃO E CONFIGURAÇÃO SISTEMA DE MONITORAMENTO ZABBIX

Iremos executar a instalação dos seguintes componentes da ferramenta de monitoramento Zabbix na versão 3.2 Servidor, Banco de Dados, interface Web e Agente, todos no mesmo servidor virtual (ZabbixServer). Lembrando que colocar todos esses serviços em um mesmo servidor não é uma prática recomendável em ambientes de produção. Sendo que um sistema de monitoramento eficiente precisa garantir sua disponibilidade, mesmo em situações onde vários serviços de sua infraestrutura venham a falhar, garantindo assim o seu propósito de monitoramento (DRILLING, 2012). Como neste trabalho o objetivo não é apresentar um sistema de monitoramento tolerante a falhas, utilizaremos da estratégia de implementação mais simples e fácil, que atenda às nossas necessidades. Temos três formas de obter o sistema

de monitoramento Zabbix; através de pacotes de distribuição, código fonte ou o virtual appliance (ZABBIX SIA, 2017), utilizaremos da primeira opção.

4.4.1 Instalação do banco de dados

O banco de dados que será instalado é o MariaDB na versão 15.1, que é uma versão desenvolvida pela comunidade do MySQL. Então no Shell da VM "ZabbixServer", crie um arquivo com o nome de "MariaDB.repo" dentro do diretório "/etc/yum.repos.d/", esse arquivo deverá receber o texto conforme apresentado no Quadro 4.2, a seguir:

Quadro 4.2 – Conteúdo do arquivo "MariaDB.repo"

```
# MariaDB 10.2 CentOS repositor list – created 2017-08-04 03:43 UTC
# http://downloads.mariadb.org/mariadb/repositories/
[mariadb]
name = MariaDB
baseurl = http://yum.mariadb.org/10.2/centos7-amd64
gpgkey=https://yum.mariadb.org/RPM-GPG-KEY-MariaDB
gpgcheck=1
```

Fonte: (MARIADB Foundation, 2017).

Durante este trabalho será necessário criar e ou alterar alguns arquivos de configuração. Isso poderá ser realizado através de editores, como "vi" ou "vim" ou através de comandos que criem, injetem ou alterem arquivos e seu conteúdo, como "echo" e ou "sed". Utilizaremos da segunda estratégia, executando os comandos apresentados no Quadro 4.3, para criar e alterar o arquivo "MariaDB.repo". Caso você ainda não tenha criado, cuidado se for copiar e colar os comandos no terminal, poderá existir divergências que costumam ser difíceis de identificar. Recomendamos que digite os comandos diretamente do terminal.

Quadro 4.3 – Comandos de criação do arquivo "MariaDB.repo"

```
# echo "# MariaDB 10.2 CentOS repositor list – created 2017-08-04 03:43 UTC" >
/etc/yum.repos.d/MariaDB.repo
# echo "# http://downloads.mariadb.org/mariadb/repositories/" >>
/etc/yum.repos.d/MariaDB.repo
```

```
# echo "[mariadb]" >> /etc/yum.repos.d/MariaDB.repo
# echo "name = MariaDB" >> /etc/yum.repos.d/MariaDB.repo
# echo "baseurl = http://yum.mariadb.org/10.2/centos7-amd64" >>
/etc/yum.repos.d/MariaDB.repo
# echo "gpgkey=https://yum.mariadb.org/RPM-GPG-KEY-MariaDB
" >> /etc/yum.repos.d/MariaDB.repo
# echo "gpgcheck=1" >> /etc/yum.repos.d/MariaDB.repo
```

Fonte: baseado em (MARIADB Foundation, 2017) e (MOTA FILHO, 2012).

Após a criação do arquivo "MariaDB.repo", podemos realizar a instalação do SGDB MariaDB, executando em sequência dos comandos apresentados no Quadro 4.4.

Quadro 4.4 – Comandos de instalação e inicialização do MariaDB

```
# yum search mariadb
# yum install MariaDB-server.x86_64 MariaDB-client.x86_64 -y -y
# systemctl start mariadb.service
# systemctl enable mariadb.service
```

Fonte: baseado em (BARTHOLOMEW, 2013) e (MARIADB Foundation, 2017).

Neste momento temos nosso servidor de banco de dados instalado, iniciado e habilitado para subir junto com o SO

4.4.2 Instalação dos componentes: Servidor, interface Web e agente

Para instalação desses três componentes, executaremos em sequência os comandos listados no Quadro 4.5.

Quadro 4.5 - Comandos de instalação das funcionalidades do Zabbix

```
# rpm -ivh http://repo.zabbix.com/zabbix/3.2/rhel/7/x86_64/zabbix-release-3.2-
1.el7.noarch.rpm
# yum search zabbix
# yum install zabbix-server-mysql.x86_64 zabbix-web-mysql.noarch zabbix-
agent.x86_64 net-tools.x86_64 -y –y
```

Fonte: baseado em (ZABBIX SIA, 2017).

Apesar do parâmetro "-y" estar incluso no comando, talvez seja necessário que você digite "y" seguido de um "Enter". Caso isso ocorra algumas vezes durante os processos de instalação, você já sabe o que fazer. Outro detalhe caso você resolva contrariar a recomendação apresentada no final do segundo parágrafo da seção 4.4.1, copiando e colando os comandos, redigite sempre as aspas (") e os parâmetros de comandos, como "-y".

4.4.3 Configuração dos componentes

Após a instalação dos componentes (banco, servidor, interface web e agente), iremos executar as configurações mínimas necessárias para iniciarmos a ferramenta de monitoramento Zabbix. Começaremos executando alguns ajustes no banco, como definir a senha de root do banco. Execute o comando do Quadro 4.6, para iniciar o processo.

Quadro 4.6 - Comando para chamar configurações do banco de dados

```
# mysql_secure_installation
```

Fonte: (BARTHOLOMEW, 2013).

Ao executar o comando, você será questionado algumas vezes, não é interesse deste trabalho explicar os questionamentos, mas sim informar como deve proceder a cada um: No primeiro tecle "Enter", no segundo digite "y" e tecle "Enter" e em seguida digite a senha que deseja atribuir ao usuário root (esse root tratado aqui é do banco de dados e não do sistema), tecle "Enter", digite novamente a senha para confirmar e tecle "Enter", nos próximos quatro questionamentos digite "y" e tecle "Enter", para finalizar esta etapa. Agora iremos criar a base de dados do Zabbix e conceder as permissões necessárias ao usuário Zabbix, que já fora criado automaticamente durante a instalação do componente "servidor". Execute os comandos, atentando-se aos seguintes detalhes: Após o primeiro comando você será solicitado a digitar a senha de root do banco e teclar "Enter", os comandos a partir da segunda linha, são só os apresentados após o texto "MariaDB [(none)]>".

Quadro 4.7 - Comandos para criação e permissionamento na base Zabbix

```
# mysql –u root -p
MariaDB [(none)]> create database zabbix character set utf8 collate utf8_bin;
```

```
MariaDB [(none)]> grant all privileges on zabbix.* to zabbix@localhost identified by
'zabbix';
MariaDB [(none)]> flush privileges;
MariaDB [(none)]> quit
```

Fonte: (ZABBIX SIA, 2017).

Se for copiar e colar os comandos, cuidado, pode haver divergências em caracteres e pode ser difícil a sua identificação, por isso novamente aconselhamos a digitar os comandos diretamente no terminal. Durante a instalação do servidor, vários arquivos foram criados, um deles é o "create.sql.gz", que está localizado no diretório "/usr/share/doc/zabbix-server-mysql-3.2.7/" que será usado nesta etapa na criação do esquema do banco Zabbix, através dos comandos do Quadro 4.8. Lembre-se que após o comando da segunda linha, será solicitado a senha do usuário Zabbix, que é simplesmente "Zabbix".

Quadro 4.8 - Comandos para criação do esquema do banco Zabbix

```
# cd /usr/share/doc/zabbix-server-mysql-3.2.7/
# zcat create.sql.gz | mysql -u zabbix zabbix -p
```

Fonte: (ZABBIX SIA, 2017).

Pronto, neste momento já temos nosso banco de dados instalado e configurado, vamos então agora alterar o arquivo "zabbix_server.conf" do componente servidor, que está localizado no diretório "\etc\zabbix\", este é o coração do servidor Zabbix e contém diversos parâmetros para o seu funcionamento, iremos configurar somente os parâmetros necessários para atender ao nosso trabalho, mas você pode e deve dedicar um tempo para o estudo e compreensão dos parâmetros desse arquivo, assim como de outros arquivos que este trabalho venha a citar. Como medida de boas práticas e segurança, iniciaremos criando uma cópia do arquivo antes de alterá-lo, execute os comandos do Quadro 4.9, a seguir:

Quadro 4.9 - Comandos para backup do arquivo "zabbix_server.conf"

```
# cd /etc/zabbix/
# ls -alh
# cp zabbix_server.conf zabbix_server.conf.bck
# ls –alh
```

Fonte: baseado em (MOTA FILHO, 2012).

Veja que agora você já tem uma cópia do arquivo original, que poderá usar para comparar ou para rollbak em caso de desastre, temos duas formas de executar as alterações necessárias, uma seria editando o arquivo através de um editor de texto como o "vi", a outra forma é através do comando "sed", que será utilizada aqui, conforme apresentado no Quadro 4.10.

Quadro 4.10 - Comandos para edição do arquivo "zabbix_server.conf"

```
# sed –i s/"# DBHost=localhost"/DBHost=localhost/g /etc/zabbix/zabbix_server.conf
# sed –i s/"# DBPassword="/DBPassward=zabbix/g /etc/zabbix/zabbix_server.conf
# sed –i s/"# DebugLevel=3"/DebugLevel=3/g /etc/zabbix/zabbix_server.conf
# sed –i s/"# StartPollers=5"/StartPollers=5/g /etc/zabbix/zabbix_server.conf
# sed –i s/"# CacheSize=8M"/CacheSize=10M/g /etc/zabbix/zabbix_server.conf
```

Fonte: baseado em (MOTA FILHO, 2012) e (ZABBIX SIA, 2017).

Com os parâmetros de configuração do componente servidor alterados, iremos configurar os parâmetros de dois arquivos de configuração "zabbix.conf" e "httpd.conf" do componente Interface Web, que estão localizados nos seguintes diretórios "/etc/httpd/conf.d/zabbix.conf" e "/etc/httpd/conf/httpd.conf", também recomendamos o estudo desses dois arquivos, mas por hora execute comandos do Quadro 4.11.

Quadro 4.11 - Comandos para backup e configuração do arquivo "zabbix.conf"

```
# ls –alh /etc/httpd/conf.d/
# cp /etc/httpd/conf.d/zabbix.conf /etc/httpd/conf.d/zabbix.conf.bck
# ls –alh /etc/httpd/conf.d/
# sed –i s/"# php_value date.timezone Europe"/"php_value date.timezone America"/g
/etc/httpd/conf.d/zabbix.conf
# sed –i s/Riga/Sao_Paulo/g /etc/httpd/conf.d/zabbix.conf
# cp /etc/httpd/conf/httpd.conf /etc/httpd/conf/httpd.conf.bck
# sed –i s/"Listen 80"/"Listen 0.0.0.0:80"/g /etc/httpd/conf/httpd.conf
```

Fonte: baseado em (MOTA FILHO, 2012) e (ZABBIX SIA, 2017).

Com as configurações realizadas, vamos então ajustar o firewall para liberar a porta 80, com os comandos do Quadro 4.12.

Quadro 4.12 - Comandos para liberar o serviço "http" no firewall

```
# firewall-cmd --permanent --add-service=http
# firewall-cmd –reload
```

Fonte: (ELLINGWOOD, 2015).

Podemos iniciar os serviços e colocá-los em modo de inicialização automática, isso é feito com os comandos do Quadro 4.13.

Quadro 4.13 - Comandos para iniciar e habilitar o serviço na inicialização

```
# systemctl start zabbix-server.service httpd.service
# systemctl enable zabbix-server.service httpd.service
```

Fonte: baseado em (ELLINGWOOD, 2015) e (ZABBIX SIA, 2017).

Agora vamos executar as configurações mínimas necessárias para colocar em estado operacional o agente, que também deve coletar as informações no servidor, execute os comandos do Quadro 4.14, que criam uma cópia de backup do arquivo "zabbix_agentd.conf" e na sequencia edita o parâmetro necessário, além de configurar sua inicialização automática com o SO e reiniciar o servidor.

Quadro 4.14 - Comandos para backup, configuração e inicialização do agente

```
# cp /etc/zabbix/zabbix_agentd.conf /etc/zabbix/zabbix_agentd.conf.bck
# sed –i s/"Hostname=Zabbix server"/Hostname=ZabbixServer/g
/etc/zabbix/zabbix_agentd.conf
# systemctl start zabbix-agent.service
# systemctl enable zabbix-agent.service
# reboot
```

Fonte: baseado em (MOTA FILHO, 2012) e (ZABBIX SIA, 2017).

Assim que a VM terminar o processo de "reboot", verifique se as configurações mínimas necessárias ao funcionamento da ferramenta de monitoramento Zabbix estão de acordo, executando os seguintes comandos do Quadro 4.15 e verificando os resultados de cada linha de comando, nas Figura 4.3, 4.4, 4.5, 4.6 subsequentes.

Quadro 4.15 - Comandos de verificação de configuração

```
# systemctl list-unit-files | grep –e firewall –e httpd –e mysql –e selinux –e Zabbix
# netstat –anp | grep ":80"
# cat /etc/selinux/config | grep SELINUX=disabled
# systemctl status mysql.service zabbix-server.service httpd.service | grep –e Active: -e
CGroup:
```

Fonte: baseado em (MOTA FILHO, 2012), (HED HAT, s.d.) e (ELLINGWOOD, 2015).

Figura 4.3 - Status dos serviços que inicializam com o SO.

```
[root@ZabbixServer ~]# systemctl list-unit-files | grep -e firewall -e httpd -e mysql -e selinux -e zabbix
firewalld.service                           enabled
httpd.service                               enabled
mysql.service                               enabled
mysqld.service                              enabled
selinux-policy-migrate-local-changes@.service static
zabbix-agent.service                        enabled
zabbix-server.service                       enabled
[root@ZabbixServer ~]#
```

Fonte: própria.

Figura 4.4 - Status da porta 80 TCP.

```
[root@ZabbixServer ~]# netstat -anp | grep ":80"
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      770/httpd
[root@ZabbixServer ~]#
```

Fonte: própria.

Figura 4.5 - Status do SELINUX.

```
[root@ZabbixServer ~]# cat /etc/selinux/config | grep SELINUX=disabled
SELINUX=disabled
[root@ZabbixServer ~]#
```

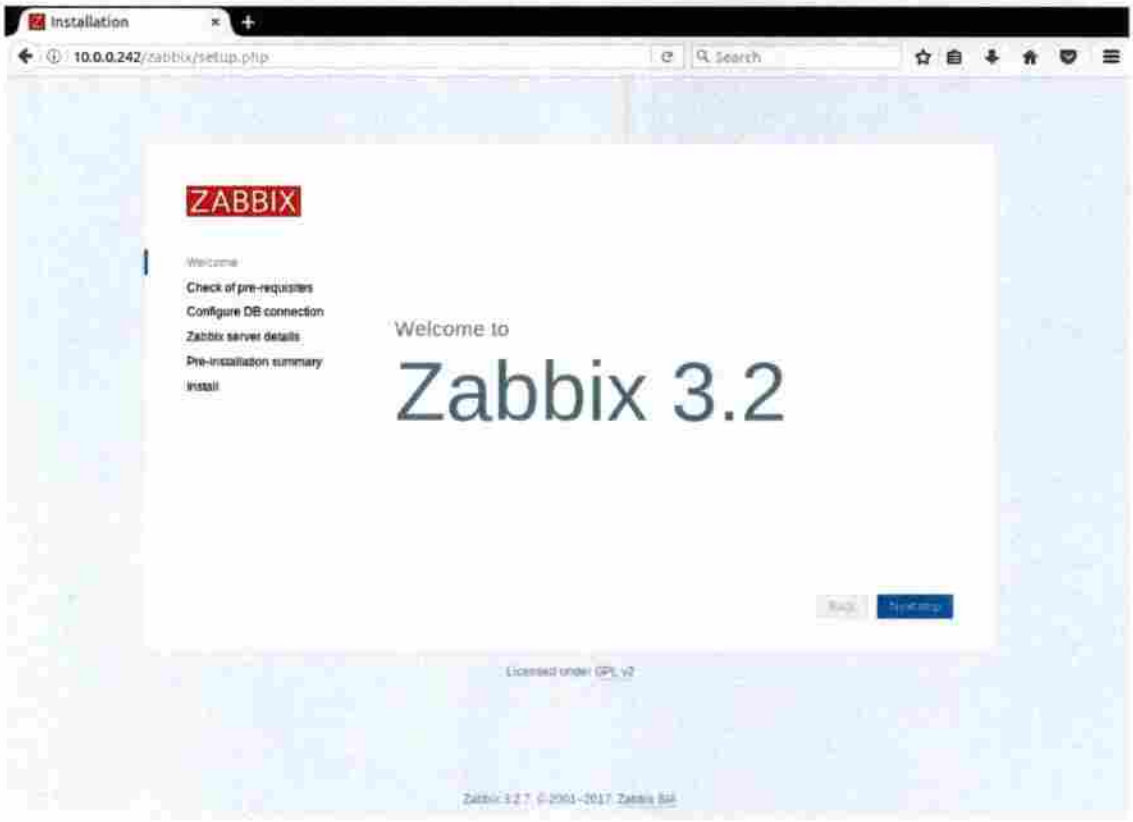
Fonte: própria.

Figura 4.6 - Status dos serviços.

Fonte: própria.

Nesse momento estamos preparados para executar o restante das configurações da ferramenta, através de um navegador que tenha acesso a rede desse servidor, entre com a url: http://10.0.0.242/zabbix no seu browser e tecle "Enter", se todos os procedimentos descritos até esse momento foram cumpridos com sucesso, você será confrontado com a Figura 4.7.

Figura 4.7 – Captura da tela de boas-vindas do Zabbix.

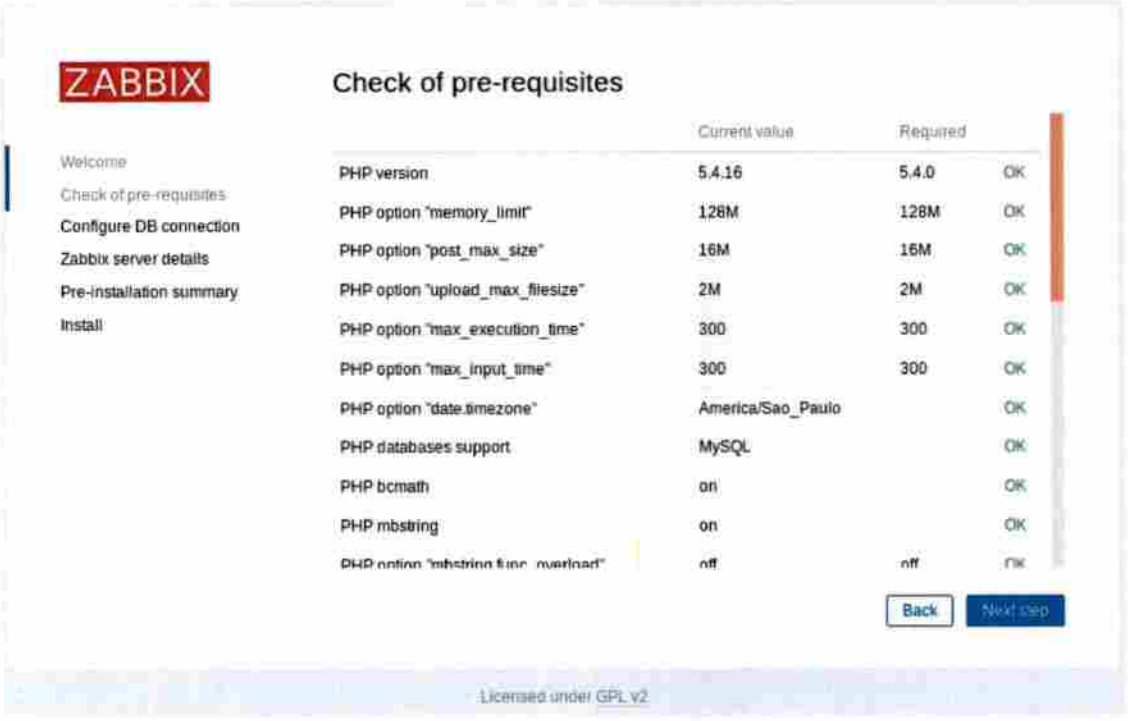


Fonte: própria.

Clique em "Next step", para passar a próxima tela, que deverá ser igual a apresentada na Figura 4.8, onde deve ser verificado se os valores ativos da segunda coluna "Current value",

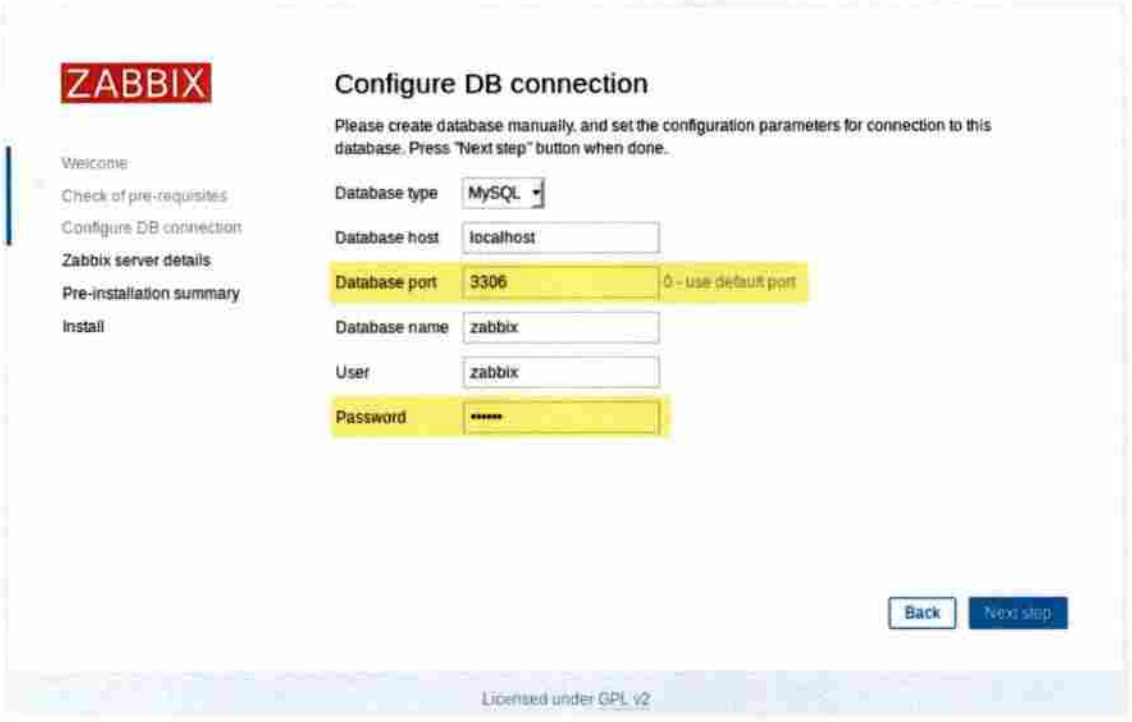
atendem, ou são superiores aos valores mínimos necessários da terceira coluna "Required", para dar sequência ao processo de instalação, estando tudo "OK"! Clique em "Next Step", para ver a Figura 4.9.

Figura 4.8 – Captura de tela de verificação dos requisitos.



Fonte: própria.

Figura 4.9 – Captura de tela de configuração de conexão com o banco de dados.



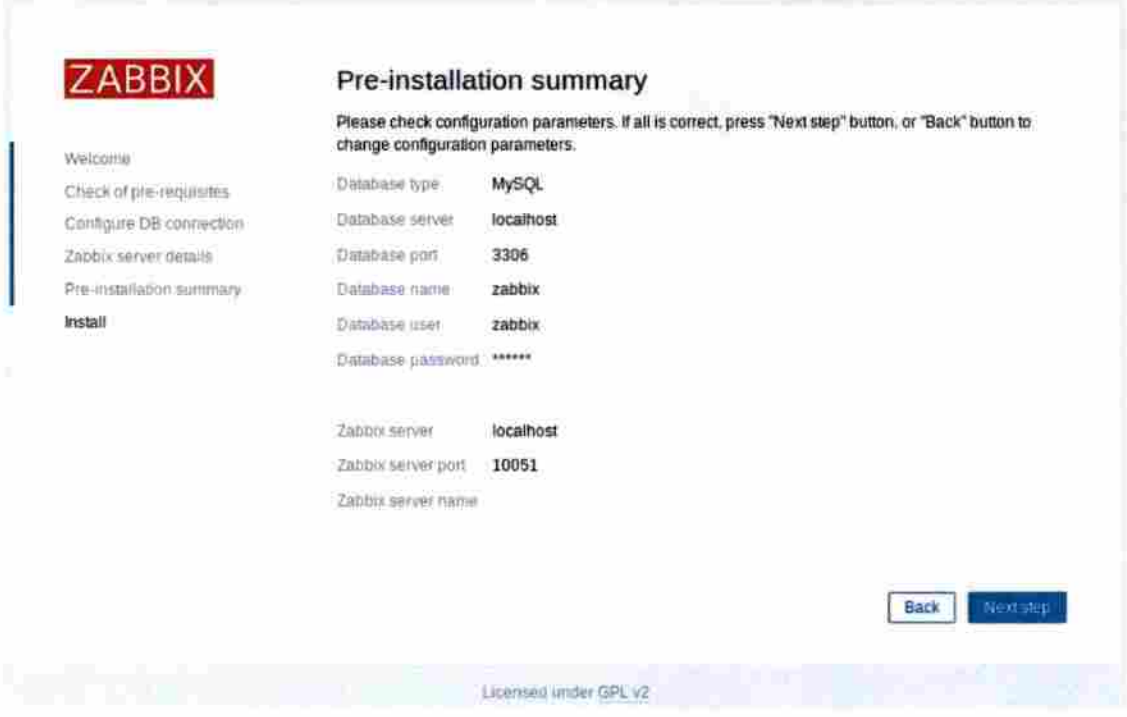
Fonte: própria.

Aqui na Figura 4.9 você pode verificar os campos relacionados a conexão da aplicação Zabbix com o banco de dados, sendo que apenas dois campos devem ser tratados na nossa instalação, que são: "Database port" que pode ser deixada como "0" ou "3306" que é a padrão do MySql, sendo também o zero considerado na configuração como porta padrão, o outro campo é o "Password" que deve ser informado o utilizado e configurado no banco e no arquivo de configuração do servidor que é "Zabbix", clique em "Next step" para dirigir-se a próxima tela, que é da Figura 4.10, onde não haverá alteração, apenas clique em "Next step", para que a próxima tela seja apresentada, conforme a Figura 4.11.

Figura 4.10 – Captura de tela de configuração de detalhes do servidor.

Fonte: própria.

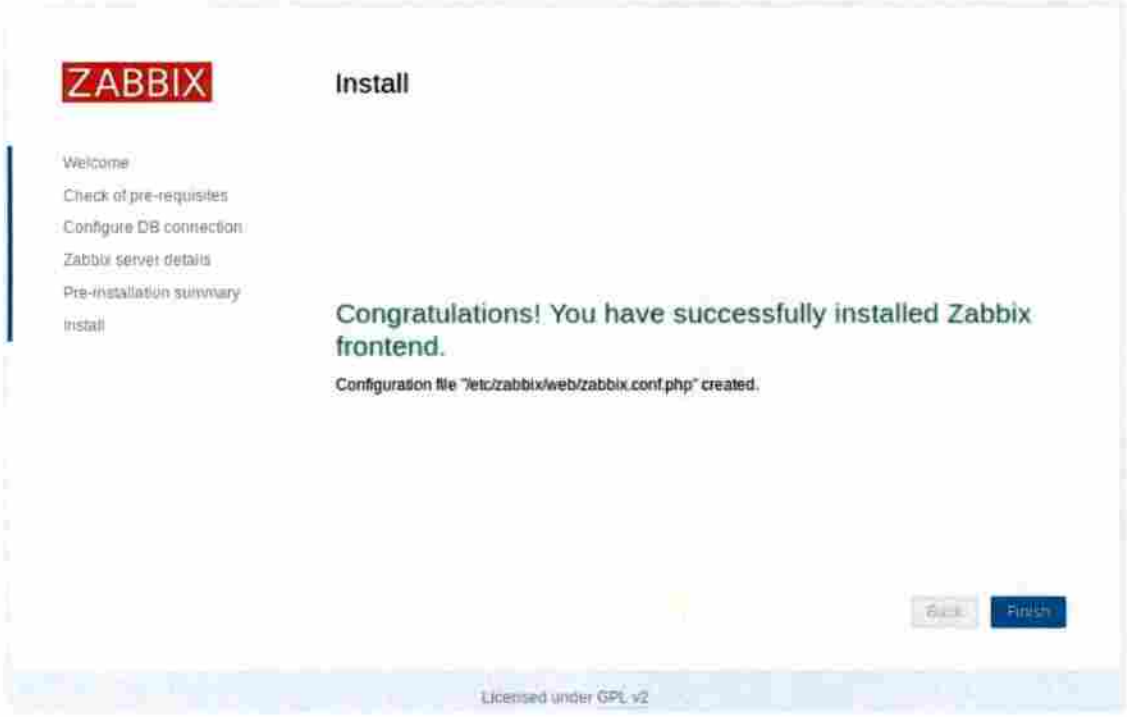
Figura 4.11 – Captura de tela com resumo das configurações.



Fonte: própria.

Verifique o resumo das configurações na Figura 4.11 e clique em "Next step", para passar a Figura 4.12.

Figura 4.12 – Captura de tela final com localização do arquivo "zabbix.conf.php".



Fonte: própria.

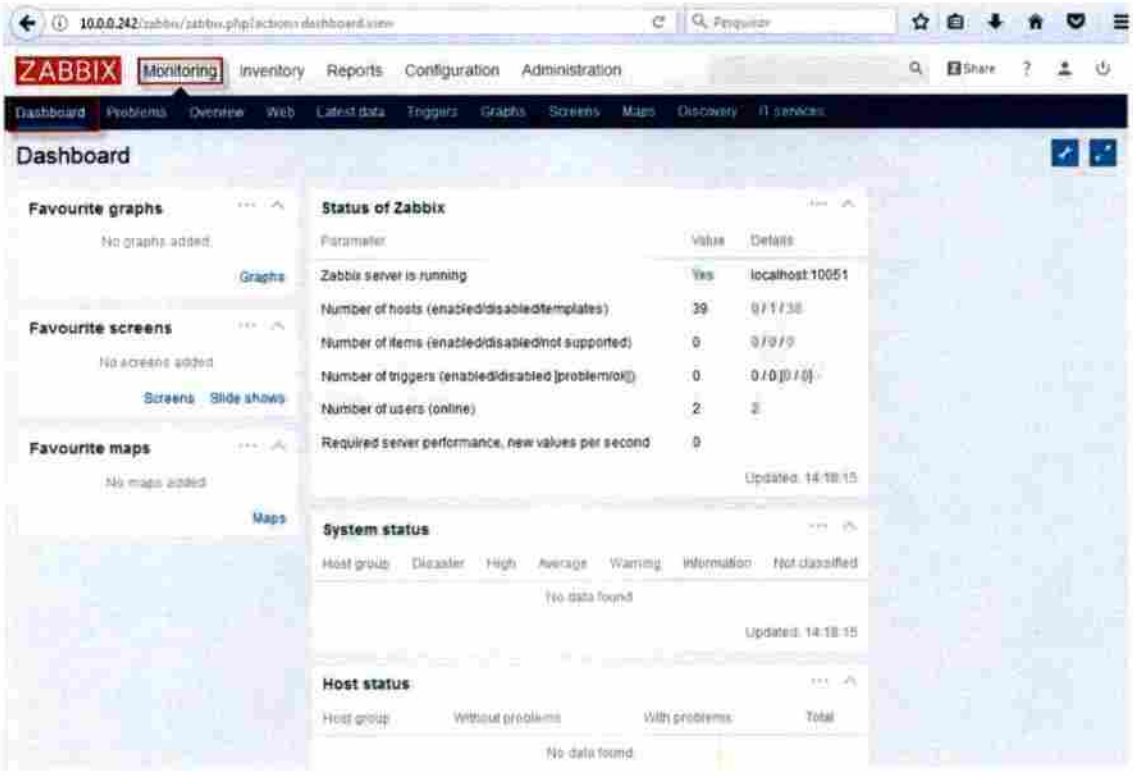
Será informado na Figura 4.12, que obteve sucesso na instalação e que fora criado o arquivo de configuração "zabbix.conf.php" no diretório "/etc/zabbix/web", clique em "Finsh" e será apresentada a tela de login, conforme Figura 4.13.

Figura 4.13 – Captura de tela de login.

Fonte: própria.

Você deve inserir o nome de usuário "Admin" e senha "Zabbix", que são padrões da instalação. Lembre-se que o Linux faz diferenciação entre caracteres maiúsculos e minúsculos, então atenção, após o login você será direcionado a tela do "Dashboard" em "Monitoring" Figura 4.14, como primeira medida vamos ativar o monitoramento do próprio servidor, seguindo os procedimentos; clique em "Configuration", "Hosts", verifique que o único host cadastrado é o "ZabbixServer", mas que está desativado "Disabled", conforme visto na Figura 4.15, clique sobre a palavra "Disabled" e será questionado a ativar ou não, conforme Figura 4.16, clique em "OK", nesse momento o servidor passa a ser monitorado Figura 4.17.

Figura 4.14 – Captura de tela inicial "Dashboard" do Zabbix.



Fonte: própria.

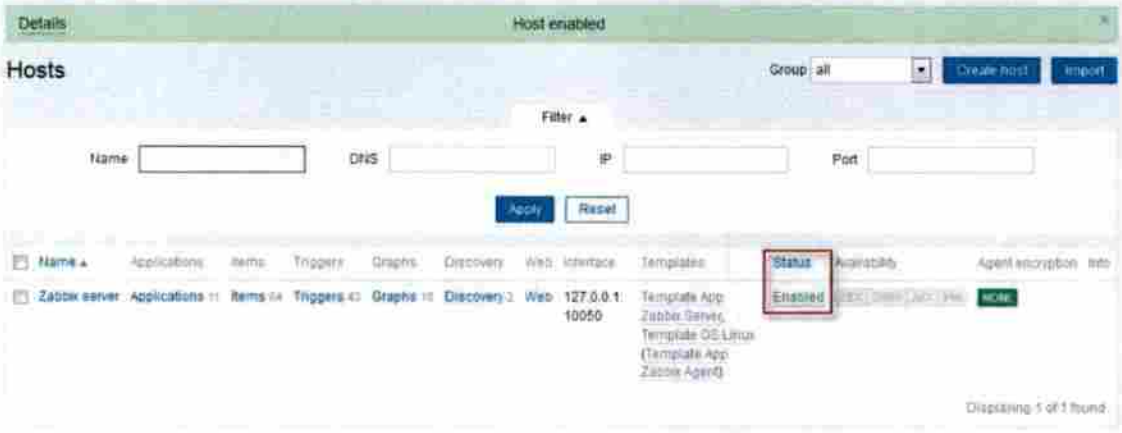
Figura 4.15 – Captura de tela, Status do host.

Fonte: própria.

Figura 4.16 – Captura de tela para confirmar alteração.

Fonte: própria.

Figura 4.17 – Captura de tela com resultado da alteração.



Fonte: própria.

Neste momento seu serviço de monitoramento já está instalado e configurado para monitorar o próprio servidor, então podemos seguir para a instalação do agente no servidor ADDS, sendo necessário alguns ajustes que nunca deverão ocorrer em ambiente que não seja de laboratório, como o nosso, pois essas configurações irão baixar consideravelmente a segurança no servidor e só estamos adotando essas medidas para facilitar nosso trabalho e não nos prolongarmos demasiadamente, cansando o leitor. Começaremos desativando o Firewall do Windows para que quando o agente seja iniciado suas portas TCP não sejam bloqueadas, pressione a tecla "Windows" e toque na Tecla "R", para que a janela do executar (Run) seja apresentada, digite a palavra "control" e tecle "Enter" ou clique em "OK" Figura 4.18, no painel de controle clique no ícone do "Windows Firewall" Figura4.19, depois clique em "Turn Windows Firewall on or off" Figura 4.20, desative o firewall em todas as redes conforme apresentado na Figura 4.21 e clique em "OK", pronto o firewall do Windows está

desativado em todas as redes, para esse servidor Figura 4.22, outro detalhe é que será necessário a execução de scripts do PowerShell. Na versão do Microsoft Windows Server 2003 a Microsoft introduziu um mecanismo de segurança que por padrão visa impedir a execução indevida de scripts do PowerShell (*.ps1) (RAMOS, 2015), sendo mantido esses mecanismos em versões posteriores, você pode ler o ártico da citação anterior, na integra, que é muito interessante e foi utilizado na próxima configuração. Pelo motivo já apresentado será necessário a execução da atividade que liberará a execução do script do PowerShell, vá em pesquisar no servidor e digite "PowerShell" Figura 4.23, clique com o botão direito do mouse sobre "Windows PowerShell ISE", depois clique em "Run as administrator" Figura 4.24, será apresentada a janela do PowerShell então clique em "Show Script Pane Top" e depois digite o seguinte comando "Set-ExecutionPolicy Bypass", clique em "run script" ou pressione a tecla "F5" e você será questionado sobre a alteração, clique em "Yes", como mostra a Figura 4.25, pronto agora o agente do Zabbix não deve ter dificuldades para rodar nesse servidor.

Figura 4.18 – Captura de tela, com Janela do executar "Run".

Fonte: própria.

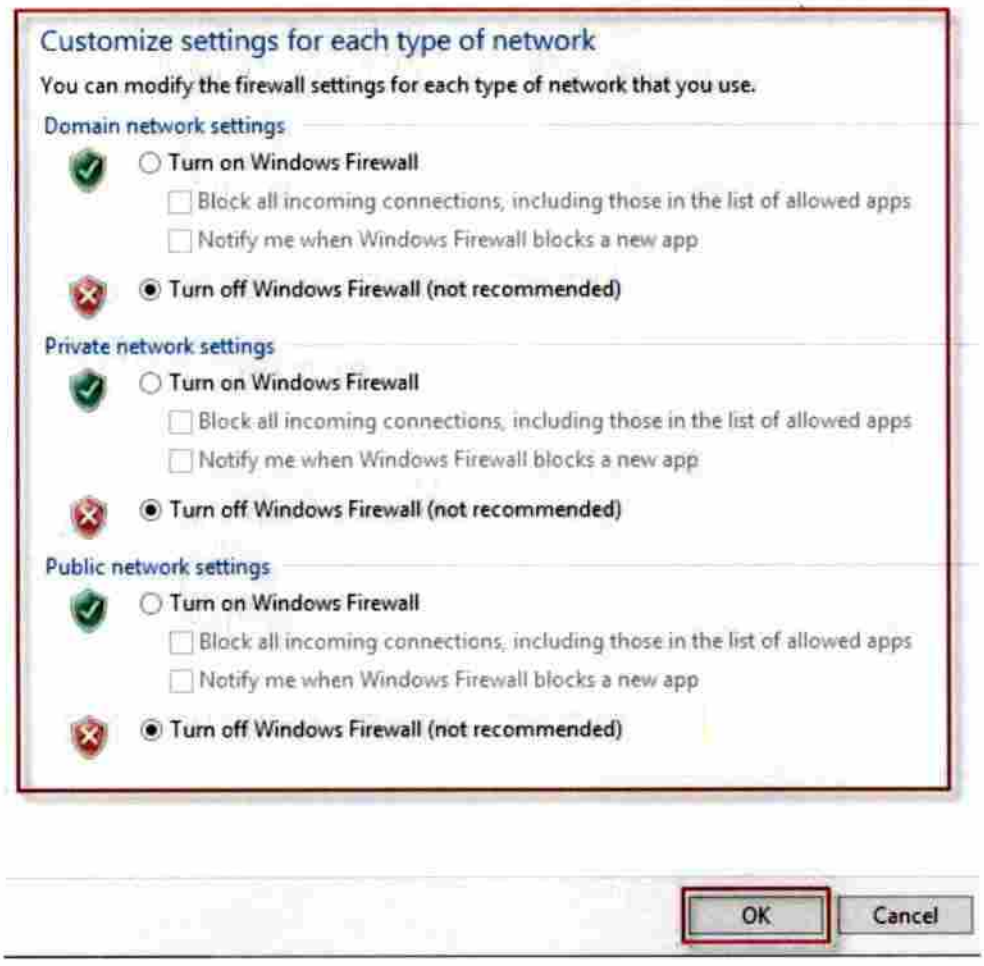
Figura 4.19 – Captura de tela, com Ícone do firewall no painel de controle.

Fonte: própria.

Figura 4.20 – Captura de tela, com ativar ou desativar firewall.

Fonte: própria.

Figura 4.21 – Captura de tela, com desativar firewall.



Fonte: própria.

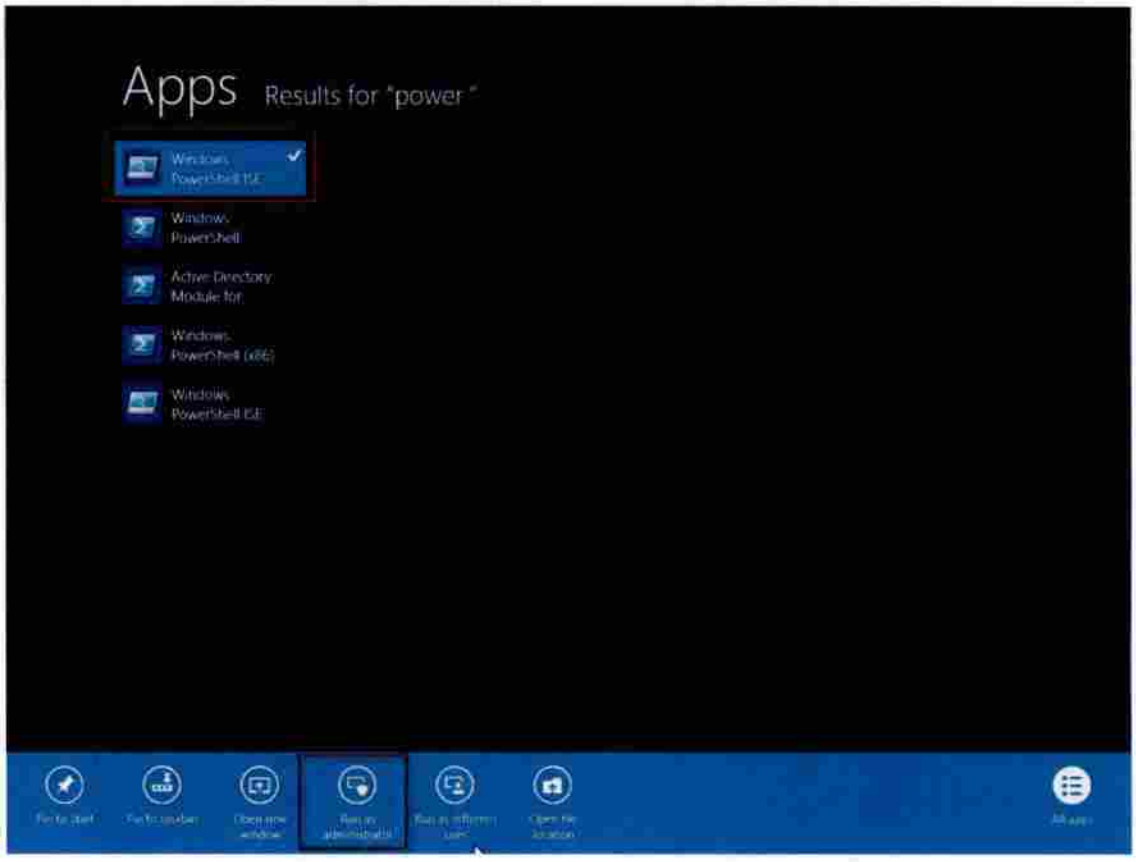
Figura 4.22 – Captura de tela, com firewall desativado, status.

Fonte: própria

Figura 4.23 – Captura de tela, com pesquisa do Windows.

Fonte: própria.

Figura 4.24 – Captura de tela, com executar como administrador.



Fonte: própria.

Figura 4.25 – Captura de tela, com janela para confirmar alteração.

Fonte: própria.

Vamos agora instalar o agente no host ADDS, sendo que existem algumas formas de instalar o agente, mas como no nosso caso esse processo será realizado em apenas um servidor Windows, seria lógico optarmos pela instalação direta e manual, mas como pode existir a necessidade de executar várias vezes o mesmo processo, então acreditamos que vale a pena

construirmos dois scripts (*.bat), um para instalar o agente e outro para removê-lo, definido isso podemos baixar (donwload) a versão 3.2 do agente para Windows, na Url: https://www.zabbix.com/downloads/3.2.0/zabbix_agents_3.2.0.win.zip após o download, descompacte o arquivo na raiz "C:" e renomeie o diretório descompactado para "Zabbix", use um editor de texto (Notepad) em modo administrador, para editar o arquivo "C:\zabbix\conf\zabbix_agentd.win.conf" ajustando os parâmetros iguais aos apresentados no Quadro 4.16, há vários parâmetros nesse arquivo, mas só configuraremos os necessários para nosso laboratório, após configurado, salvo o arquivo. Abra novamente o bloco de notas (Notepad) em modo administrador e digite o texto do Quadro 4.17, salve como "Instala_Agentd.bat", dentro do diretório "C:\zabbix", em seguida repita o processo anterior só que utilizando o texto informado no Quadro 4.18 e salvar o arquivo com o nome de "Remove_Agentd.bat" no mesmo diretório. O material consultado e utilizado para servir de referência na construção dos scripts de instalação e remoção do agente, fora (MOTA, 2012) , já para as configurações do arquivo "zabbix_agentd.win.conf" fora utilizado como referências (DRILLING, 2012), (HORST, PIRES, & DÉO, 2015) e (ZABBIX SIA, 2017).

Quadro 4.16 - Configuração do arquivo "zabbix_agentd.win.conf"

```
LogFile=C:\zabbix\zabbix_agentd.log
DebugLevel=3
Server=10.0.0.242
StartAgents=5
Hostname=ADDS
Timeout=15
```

Fonte: baseado em (DRILLING, 2012), (HORST, PIRES, & DÉO, 2015) e (ZABBIX SIA, 2017).

Quadro 4.17 - Script de instalação do agente Zabbix

```
@echo off
@echo. >> c:\zabbix\Instala_Agentd_Log.txt
Echo ################## INSTALA AGENTE ZABBIX ######################
>> c:\zabbix\Instala_Agentd_Log.txt
@echo. >> c:\zabbix\Instala_Agentd_Log.txt
cd\
Date /T >> c:\zabbix\Instala_Agentd_Log.txt
```

```
IF EXIST "c:\Program Files (x86)" (
c:\zabbix\bin\win64\zabbix_agentd.exe -i -c c:\zabbix\conf\zabbix_agentd.win.conf >>
c:\zabbix\Instala_Agentd_Log.txt 2>&1
) ELSE (
c:\zabbix\bin\win32\zabbix_agentd.exe -i -c c:\zabbix\conf\zabbix_agentd.win.conf >>
c:\zabbix\Instala_Agentd_Log.txt 2>&1
)
net start "zabbix Agent" >> c:\zabbix\Instala_Agentd_Log.txt 2>&1
msg * Verifique o arquivo "Instala_Agentd_Log.txt"! Registar o servidor no
monitoramento!
C:\zabbix\Instala_Agentd_Log.txt
Exit
```

Fonte: baseado em (MOTA, 2012) e (ZABBIX SIA, 2017).

Quadro 4.18 - Script de remoção do agente Zabbix

```
@echo off
@echo. >> c:\zabbix\Instala_Agentd_Log.txt
Echo ################## REMOVE AGENTE ZABBIX ######################
>> c:\zabbix\Instala_Agentd_Log.txt
@echo. >> c:\zabbix\Instala_Agentd_Log.txt
cd\
Date /T >> c:\zabbix\Instala_Agentd_Log.txt
net stop "zabbix Agent" >> c:\zabbix\Instala_Agentd_Log.txt 2>&1
IF EXIST "c:\Program Files (x86)" (
c:\zabbix\bin\win64\zabbix_agentd.exe -d -c c:\zabbix\conf\zabbix_agentd.win.conf >>
c:\zabbix\Instala_Agentd_Log.txt 2>&1
) ELSE (
c:\zabbix\bin\win32\zabbix_agentd.exe -d -c c:\zabbix\conf\zabbix_agentd.win.conf >>
c:\zabbix\Instala_Agentd_Log.txt 2>&1
)
msg * Verifique o arquivo "Instala_Agentd_Log.txt"! Desative ou Remova o servidor no
monitoramento!
C:\zabbix\Instala_Agentd_Log.txt
```

Exit

Fonte: baseado em (MOTA, 2012) e (ZABBIX SIA, 2017).

Execute como administrador o arquivo que acabou de criar "C:\zabbix\Instala_Agentd.bat", para iniciar o processo de instalação do serviço do agente, esse processo é bem rápido e se tiver executado todos os passos corretamente receberá uma mensagem igual à da Figura 4.26 e também verá o arquivo de log da instalação do agente, verifique se não houve registro de erros, estando tudo correto feche o arquivo de log e continue a configuração.

Figura 4.26 – Captura de tela, com mensagem de alerta.

Fonte: própria.

Como informado na mensagem, vamos registrar o host no sistema de monitoramento, através da interface Web, acesse a url: http://10.0.0.242/zabbix, entre com o usuário "Admin" e senha "Zabbix", siga para "Configuration", "Host groups", clique em "Create host group", conforme Figura 4.27, então será apresentada a Figura 4.28 onde deve ser informado o "Group name" que será "Domain Controller", depois clique em "Add", agora que temos o grupo vamos em "Configuration", "Hosts", clique em "Create host" e será apresentada a janela da Figura4.29, informe o "Host name" que deve ser o mesmo do host que está no arquivo de configuração do agente, no nosso caso será "ADDS", informe o "Visible name", que pode ser um nome que lhe seja mais amigável ou ajude a lembrar a função deste servidor. Selecione a qual grupo ele pertencerá, "Domain Controller", informe o "IP address" do host que está sendo cadastrador, que é "10.0.0.1" e clique em "Add", para concluir o cadastro, o resultado é mostrado na Figura 4.30, veja que o host está cadastrado, mas ainda está desativado "Disabled", clique sobre essa palavra que está em vermelho, conforme visto na

tela da figura citada anteriormente, será questionado a Ativar "Enabled" o host Figura 4.31, clique em "OK".

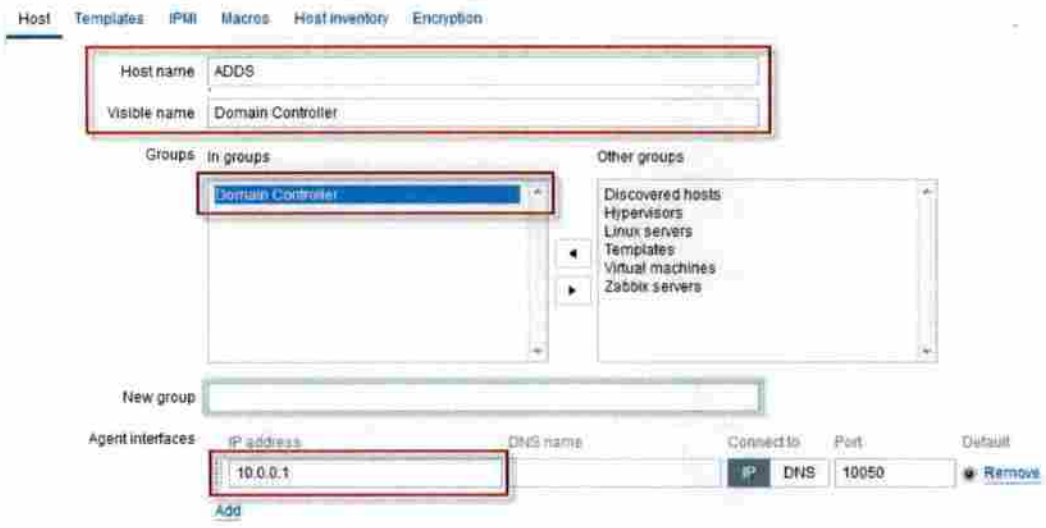
Figura 4.27 – Captura de tela de cadastro de grupo.

Fonte: própria.

Figura 4.28 – Captura de tela para adicionar o grupo.

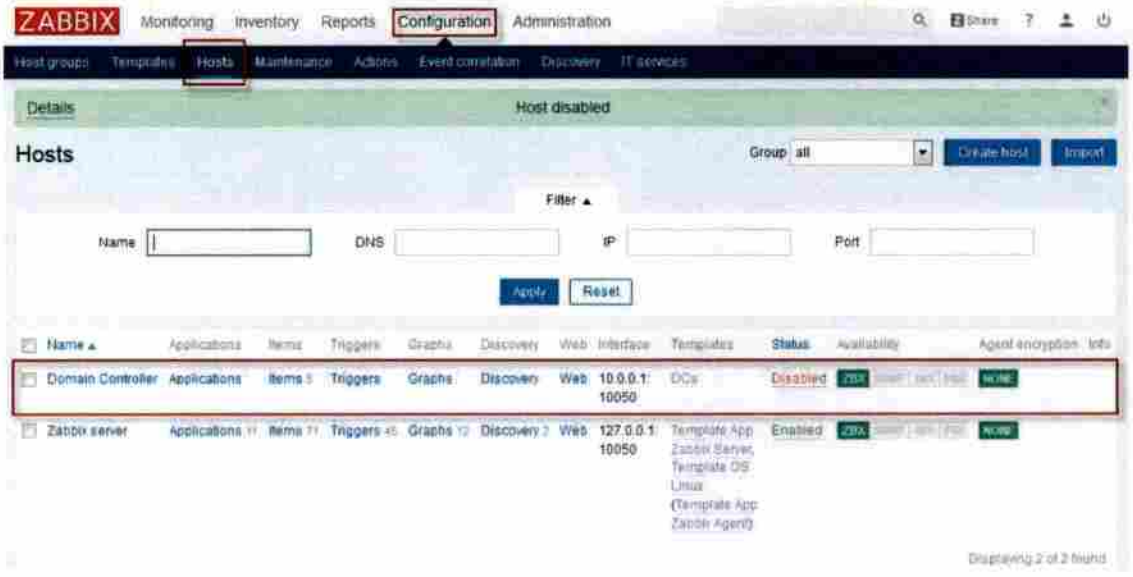
Fonte: própria.

Figura 4.29 – Captura de tela de cadastro de host.



Fonte: própria.

Figura 4.30 – Captura de tela de status de host.

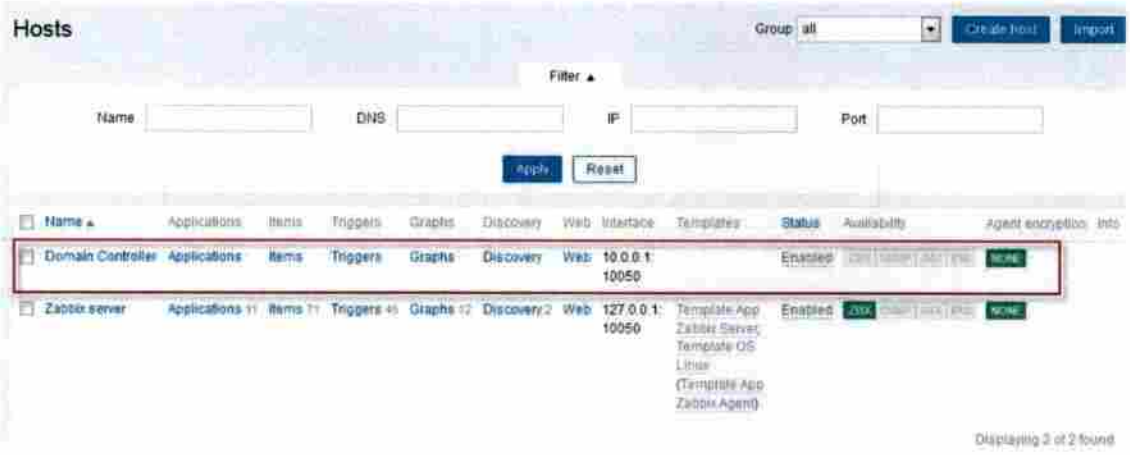


Fonte: própria.

Figura 4.31 – Captura de tela de confirmação da configuração.

Fonte: própria.

Figura 4.32 – Captura de tela de status de host, pós configuração.



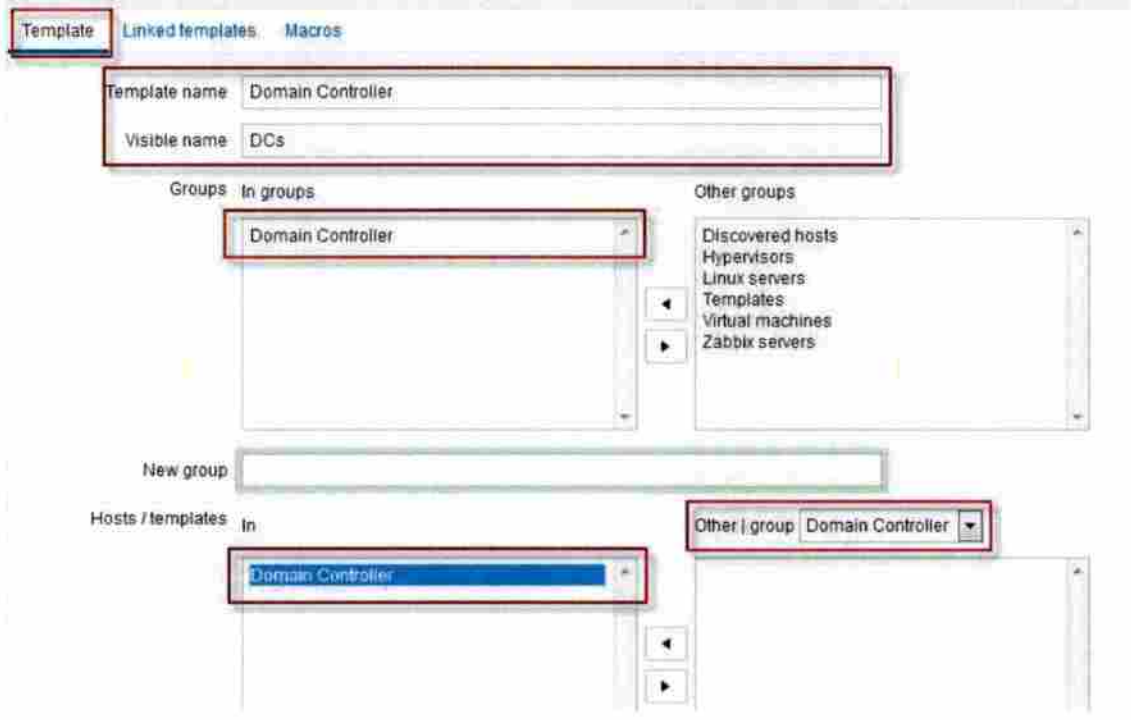
Fonte: própria.

Você com certeza notou que não foi atribuído nenhum "template" ao host cadastrado, pois a intenção é criar um "template" com os itens que desejamos monitorar, comecemos clicando em "Configuration", "Templates", clique em "create template", conforme Figura 4.33, será apresentada uma janela que deve ser preenchida igual a Figura 4.34, "Template name" igual a "Domain Controller", "Visible name" igual a "DCs", "Groups In groups" igual a "Domain Controller", "Host / template" igual a "Domain Controller", clique "Add", isso irá criar o template já o associando ao grupo correto, conforme visto na Figura 4.35.

Figura 4.33 – Captura de tela para cadastrar Templates.

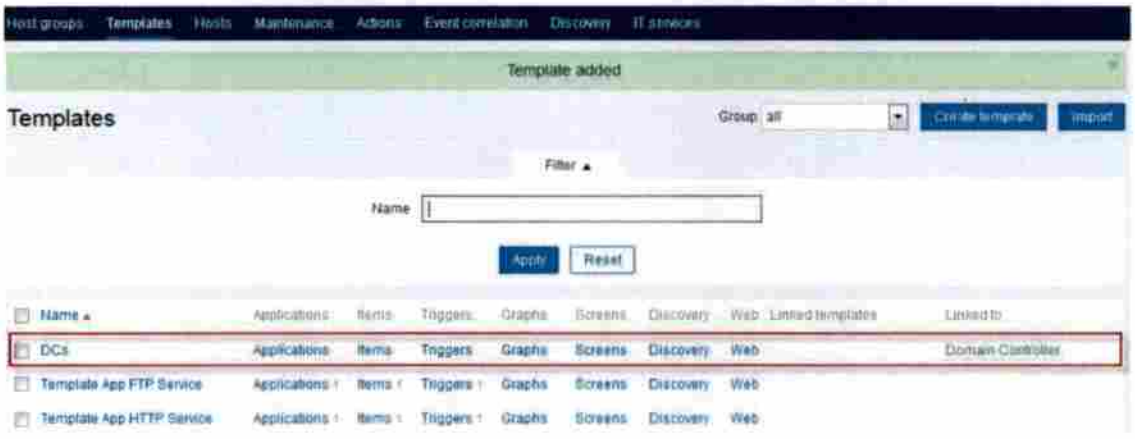
Fonte: própria.

Figura 4.34 – Captura de tela de cadastro de Template.



Fonte: própria.

Figura 4.35 – Captura de tela de status de Templates.



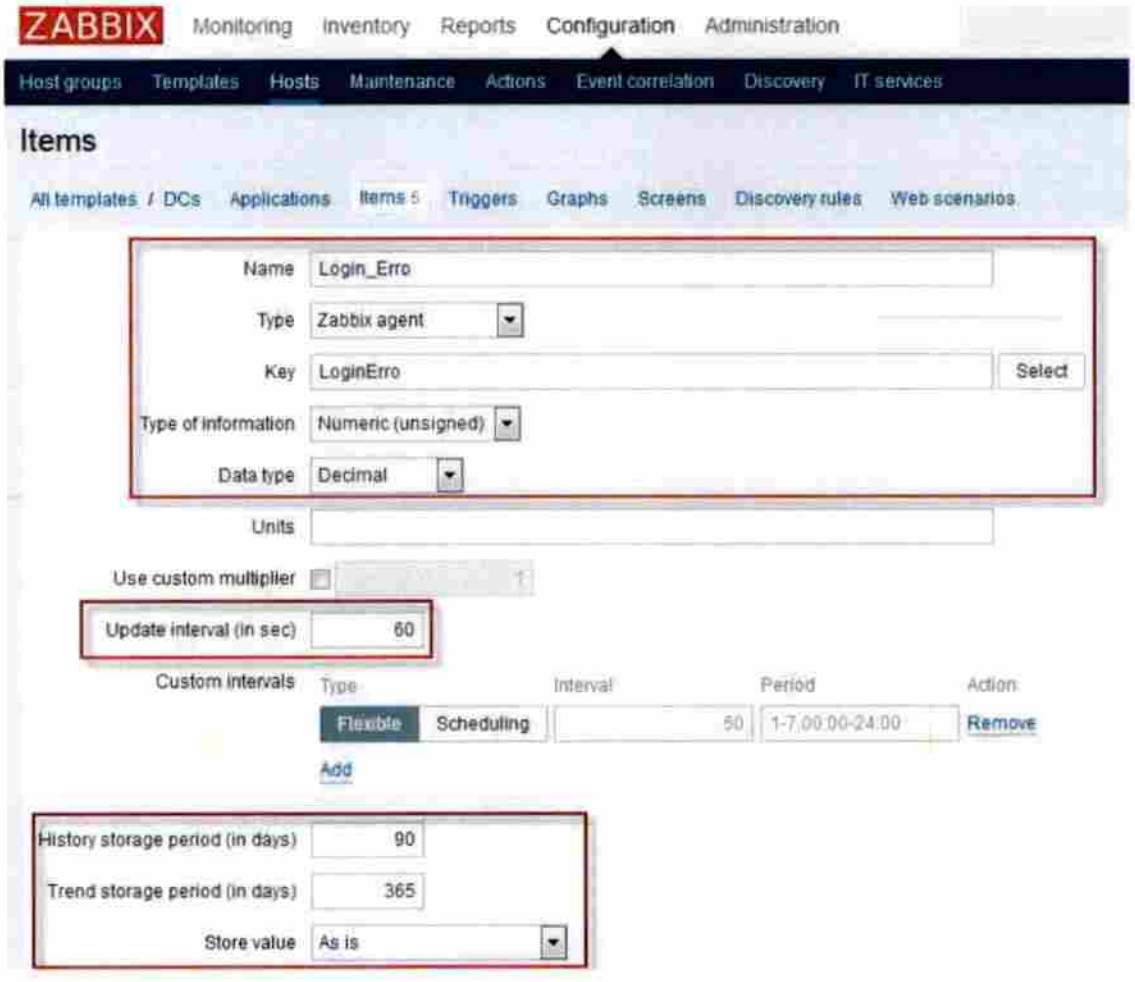
Fonte: própria.

Vamos agora criar os dois itens que nos interessam, na mesma janela da Figura 4.35, clique na palavra "Itens", que será apresentada a janela da Figura 4.36, clique em "Create item", preencha os campos conforme Figura 4.37, sendo importante mencionar que o campo "Key" deve ser o mesmo que será utilizado mais a frente (LoginErro e LoginSucesso), por nossos scripts, no final dessa janela, clique em "Add", agora clique sobre o Item que acabou de criar "LoginErro" Figura 4.38 e será apresentada novamente a janela da Figura 4.37, vá até o final da janela e clique em "Clone", isso cria uma cópia do Item onde você deve trocar apenas o "Name" para "Login_Sucesso e a "Key" para "LoginSucesso", depois no final da janela clique em "Add", caso essa opção não se apresente, cuidado você não clonou o item e sim está editando o primeiro item, então atenção, o resultado final pode ser visto na Figura 4.39, as configurações de grupos, templates, itens e hosts, foram baseadas em (HORST, PIRES, & DÉO, 2015) e (ZABBIX SIA, 2017).

Figura 4.36 – Captura de tela de criação de Itens.

Fonte: própria.

Figura 4.37 – Captura de tela de cadastro do Item.



Fonte: própria.

Figura 4.38 – Captura de tela, status do Item.

Fonte: própria.

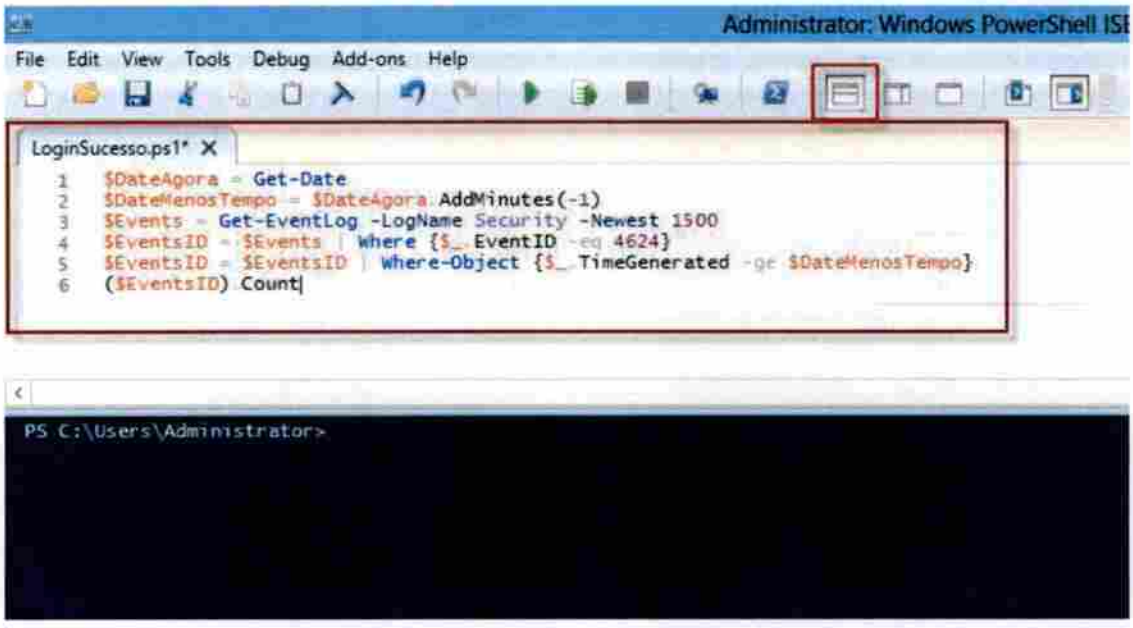
Figura 4.39 – Captura de tela com status de Itens.

Fonte: própria.

4.5 CONSTRUÇÃO DE SCRIPT DO POWERSHELL

Para que possamos contabilizar a quantidade de vezes que um determinado ID foi registrado em log do host "ADDS", em um determinado período, precisamos primeiramente saber quais Identificadores de evento (Event ID) desejamos filtrar, e para nos ajudar nessa missão utilizaremos as planilhas de referência que a Microsoft disponibiliza para download nos seguintes endereços url: http://www.microsoft.com/download/details.aspx?id=50034 e https://www.microsoft.com/en-us/download/details.aspx?id=35753 dessas planilhas foram utilizados os seguintes identificadores de eventos; "Event ID 4624, An account was successfully logged on" e "Event ID 4771, Kerberos pre-autentication failed", relacionados ao processo de logon com sucesso e falha. Agora que já temos os ID's que precisamos, vamos desenvolver dois scripts em PowerShell para filtrar o ID 4624 e 4771. Vamos começar abrindo como administrador o "Windows PowerShell ISE", então na janela do PowerShell clique em "Show Script Pane Top", e vamos digitar o conteúdo da Quadro 4.19, na parte branca da janela, como apresentado na Figura 4.40, em seguida salve o arquivo em "C:\zabbix\LoginSucesso.ps1", após salvar o primeiro arquivo abra uma nova "Aba" Figura 4.41, no PowerShell e digite o contudo da Quadro 4.20 e no final salve o arquivo em "C:\zabbix\LoginErro.ps1". Como referência no desenvolvimento dos scripts em PowerShell fora utilizado o conhecimento adquirido nas obras de; (HOLME, RUEST, RUEST, & NORTHRUP, 2009), (PAYETTE, 2008) e (MACKIN & ORION, 2016).

Figura 4.40 – Captura de tela do PowerShell.



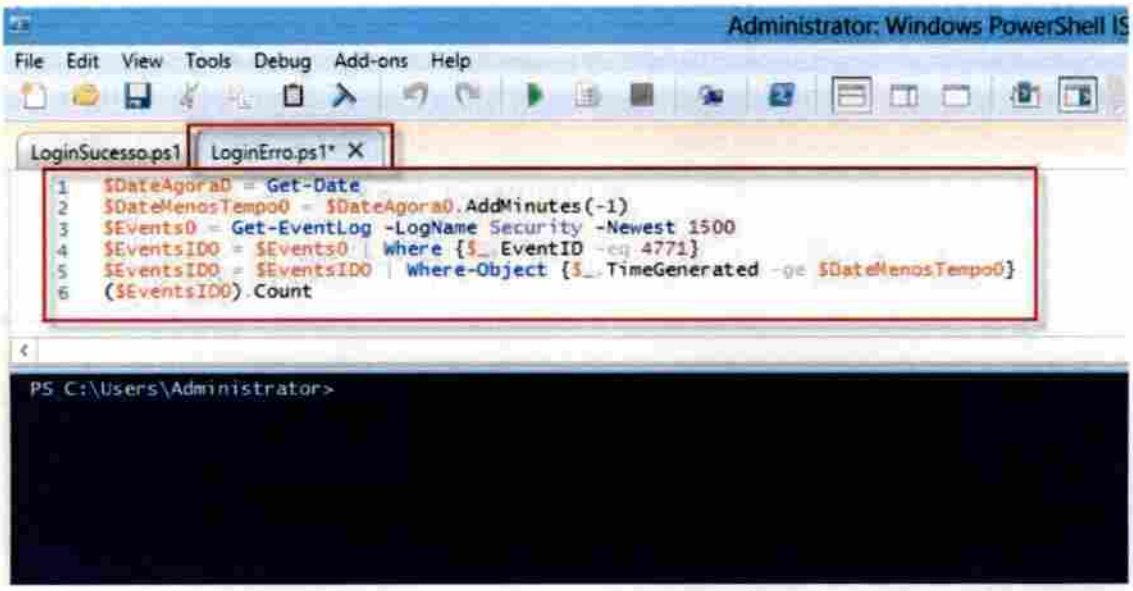
Fonte: própria.

Quadro 4.19 - Script para contabilizar ID 4624

```
$DateAgora = Get-Date
$DateMenosTempo = $DateAgora.AddMinutes(-1)
$Events = Get-EventLog –LogName Security –Newest 1500
$EventsID = $Events | Where {$_.EventID –eq 4624}
$EventsID = $EventsID | Where-Object {$_.TimeGenerated –ge $DateMenosTempo}
($EventsID).Count
```

Fonte: baseado em (PAYETTE, 2008), (HOLME, RUEST, RUEST, & NORTHRUP, 2009) e (MACKIN & ORION, 2016).

Figura 4.41 – Captura de tela do PowerShell, com aba.



Fonte: própria.

Quadro 4.20 - Script para contabilizar ID 4771

```
$DateAgora0 = Get-Date
$DateMenosTempo0 = $DateAgora0.AddMinutes(-1)
$Events0 = Get-EventLog –LogName Security –Newest 1500
$EventsID0 = $Events0 | Where {$_.EventID –eq 4771}
$EventsID0 = $EventsID0 | Where-Object {$_.TimeGenerated –ge $DateMenosTempo0}
($EventsID0).Count
```

Fonte: baseado em (PAYETTE, 2008), (HOLME, RUEST, RUEST, & NORTHRUP, 2009) e (MACKIN & ORION, 2016).

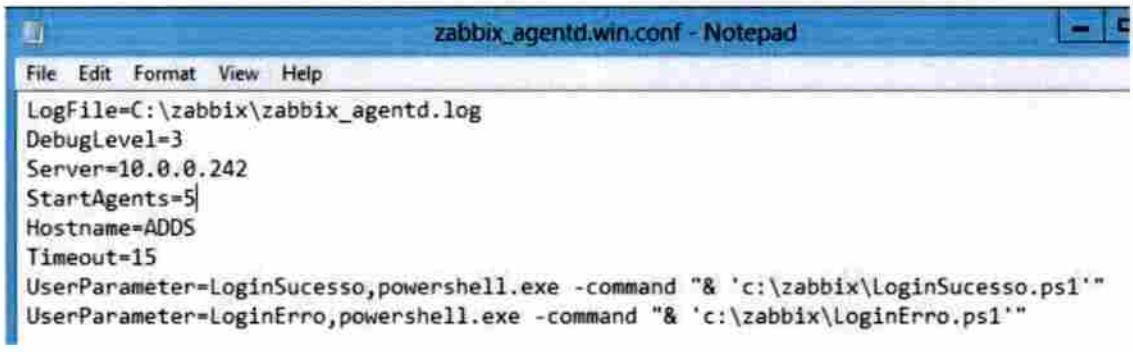
Agora vamos novamente editar o arquivo "C:\zabbix\conf", com o "NotePad" do Windows, sempre em modo administrador. Adicione as linhas contidas no Quadro 4.21, as já existentes e salve o arquivo, essa alteração irá chamar os scripts conforme itens (Login_Sucesso e Login_Erro) criados e configurados na ferramenta de monitoramento. No final o arquivo ficará igual ao da Figura 4.42.

Quadro 4.21 - Linhas adicionais do arquivo "zabbix_agentd.win.conf"

UserParameter=LoginSucesso,powershell.exe –command "& 'c:\zabbix\LoginSucesso.ps1'"
UserParameter=LoginErro,powershell.exe –command "& 'c:\zabbix\LoginErro.ps1'"

Fonte: baseado em (ZABBIX SIA, 2017).

Figura 4.42 – Captura de tela, com a configuração final do arquivo "zabbix_agentd.win.conf".



Fonte: própria.

Toda vez que alteramos o arquivo de configuração do agente, será necessário reiniciar o serviço do "zabbix Agent", para validar as alterações.

4.6 GERANDO, COLETANDO E ANALISANDO OS DADOS DE AUTENTICAÇÃO

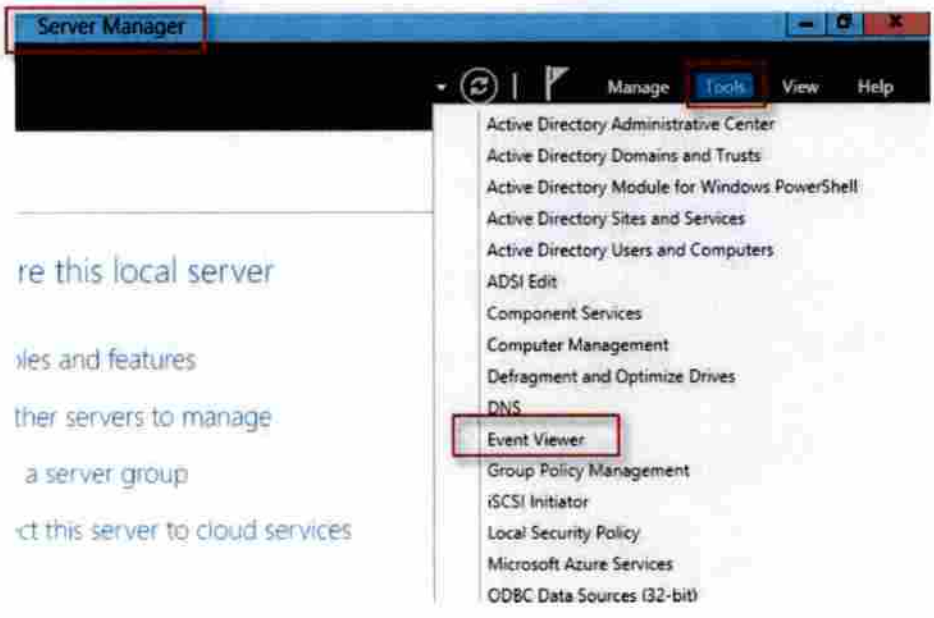
Agora que nosso ambiente foi criado e configurado vamos gerar algumas tentativas de login no host "Win7", para validar as configurações que foram executadas no item 4.3 desse trabalho; com a conta de domínio do usuário João, digitaremos a senha errada quatro vezes, gerando a tela de erro conforme a Figura 4.43 e em seguida digitaremos a senha correta, para que tanto o ID 4771 como o ID 4624, sejam registrados no log do controlador de domínio essas tentativas de autenticação, para validar isso devemos logar no host ADDS e logo no início será nos apresentada a tela do "Server Manager", onde iremos clicar em "Tools" e selecionar "Event Viewer" no menu que se apresenta, conforme visto na Figura 4.44, após esse procedimento você conseguirá visualizar a janela do "Event Viewer" onde devemos clicar com o botão contrário do mouse sobre a palavra "Security" e em seguida clicar com o botão esquerdo do mouse na opção "Filter Current Log...", no menu suspenso, conforme

Figura 4.45, agora na janela do "Filter Current Log", Figura 4.46, informe apenas o ID do evento que estamos procurando, que é o ID 4771 e clique em "OK", para aplicar o filtro, depois repita o procedimento anterior, mas informe o ID 4624 Figura 4.47, para aplicar o filtro.

Figura 4.43 – Captura de tela de login, com erro de usuário ou senha.

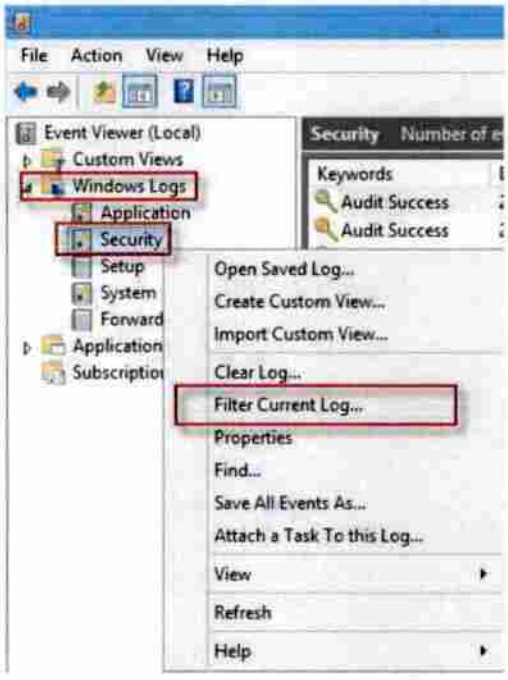
Fonte: própria.

Figura 4.44 – Captura de tela do Server Manager, acesso ao "Event Viewer".



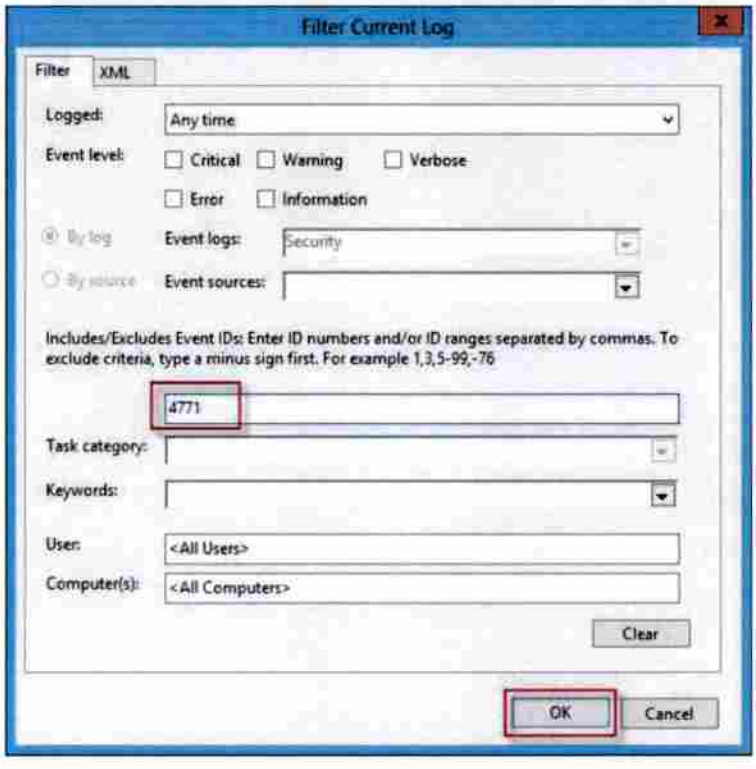
Fonte: própria.

Figura 4.45 – Captura de tela do "Filter Current Log".



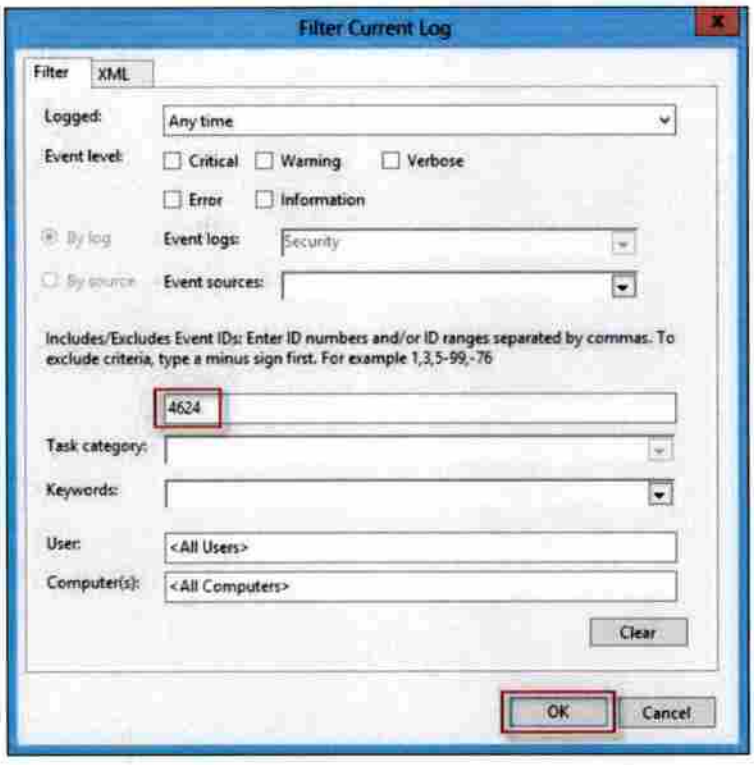
Fonte: própria.

Figura 4.46 – Captura de tela de aplicação de filtro com ID 4771.



Fonte: própria.

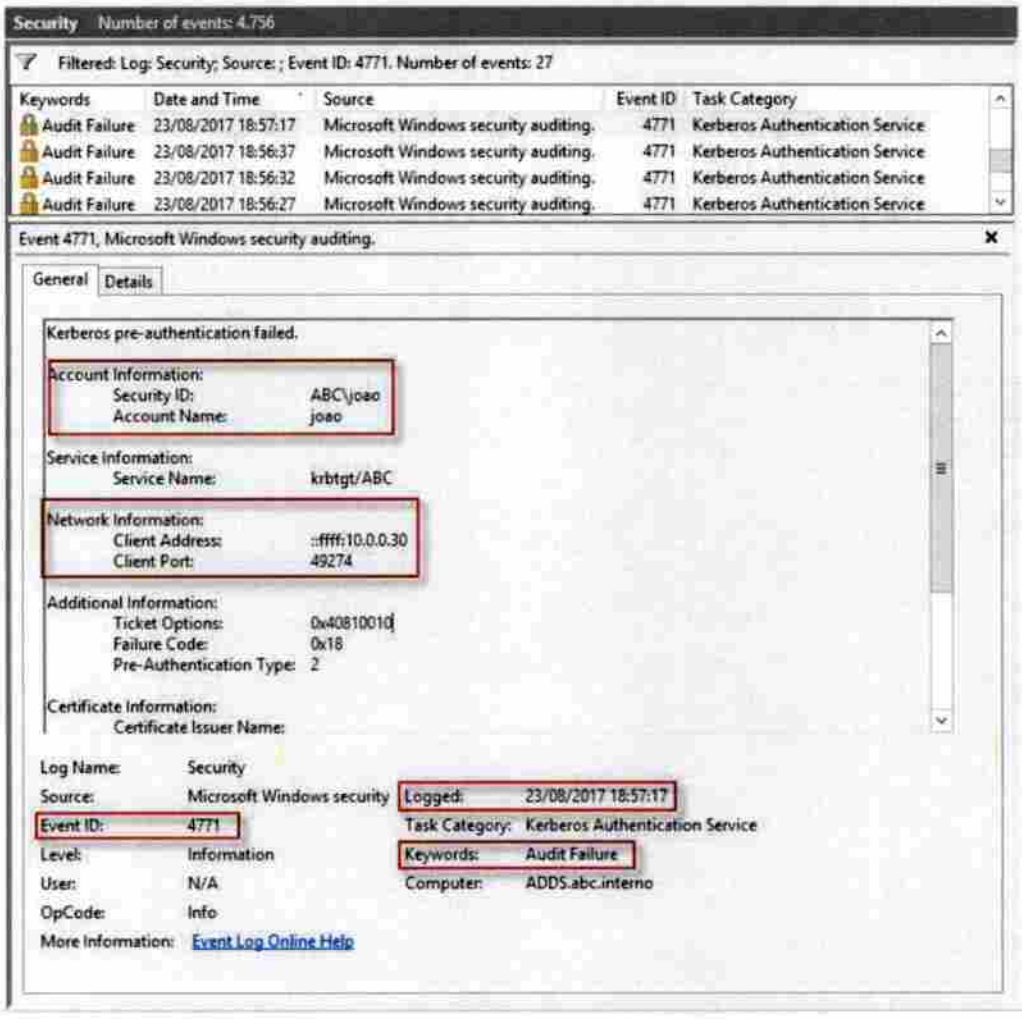
Figura 4.47 – Captura de tela de aplicação de filtro com ID 4624.



Fonte: própria.

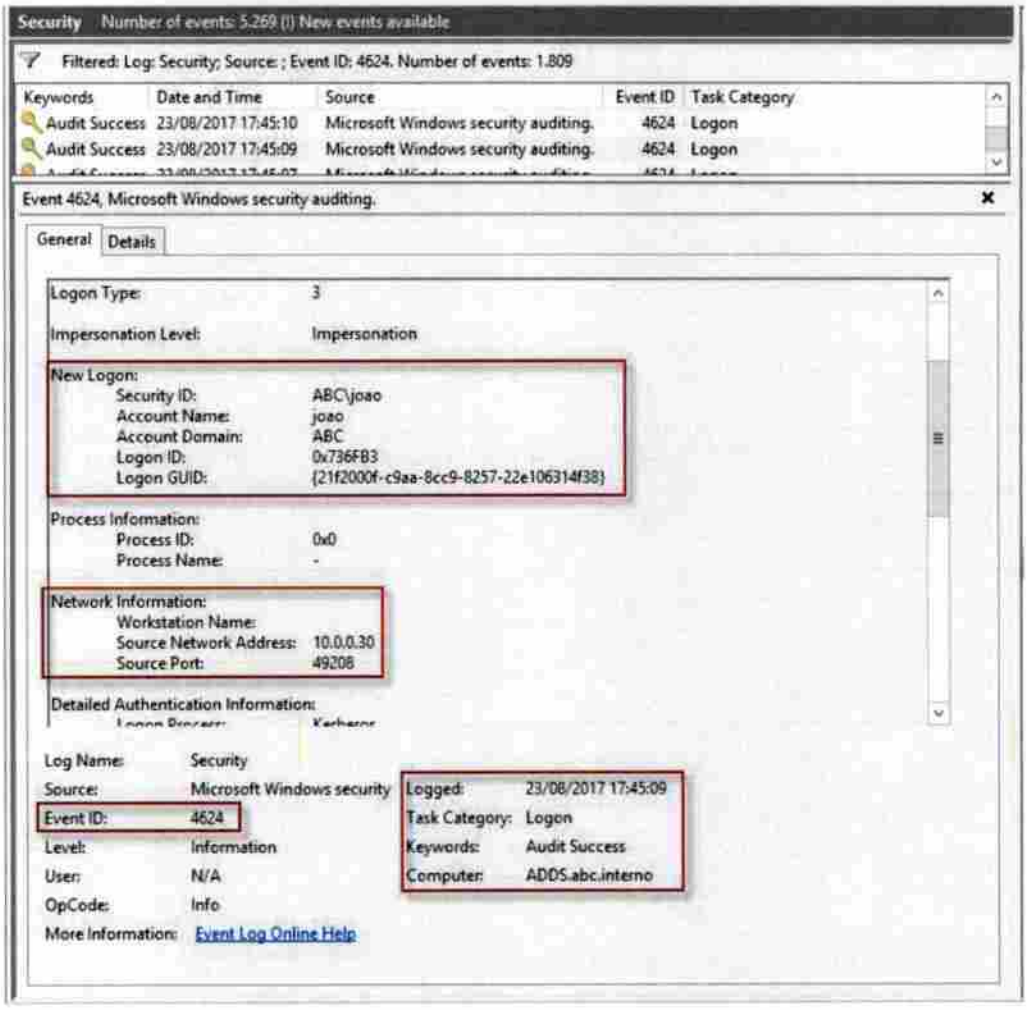
Como resultado podemos ver que os logs com o ID 4771 e 4624, foram registrados no período que tentamos autenticar o usuário "joao", informando algumas vezes a senha correta e em outras a senha errada. Podemos conferir alguns detalhes dos eventos nas Figura 4.48 e 4.49.

Figura 4.48 – Captura de tela, detalhe o usuário, IP do solicitante, evento e horário do registro.



Fonte: própria.

Figura 4.49 – Captura de tela, detalhe o usuário, IP do solicitante, evento e horário do registro.

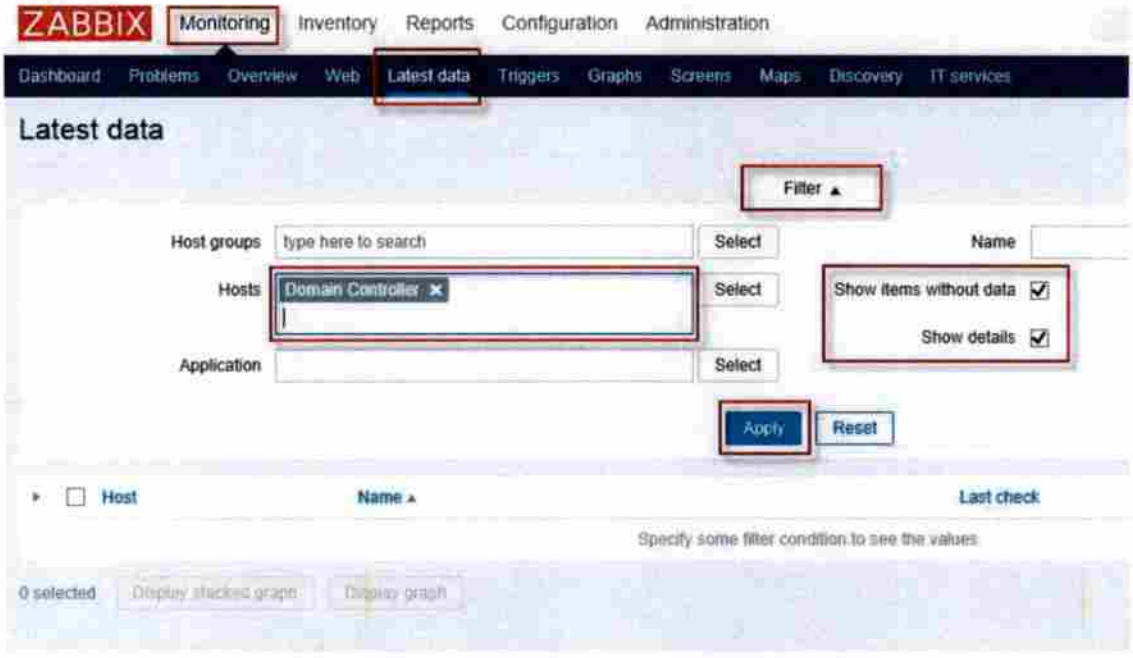


Fonte: própria.

Agora que testamos e validamos o registro em log dos ID's de eventos desejados, vamos verificar se o número de tentativas de login será coletada e armazenada pela nossa ferramenta de monitoramento. Vamos acessar novamente via navegador o Zabbix e clicar em "Monitoring", "Latest data", "Filter" e selecione "Show items without data" e "Show details", digite em "Hosts" o nome "Domain Controller", clique em "Apply", essas informações estão na Figura 4.50, já a Figura 4.51 apresenta o resultado da consulta, onde podemos ver os itens "Login_Erro" e "Login_Sucesso", no final da linha desses itens podemos ver a palavra "Graph" que vamos clicar nela para abrir outra janela com o gráfico do monitoramento do item "Login_Erro" Figura 4.52, veja que é apresentado a quantidade de erros de login em um período de 13 minutos, logo em seguida na Figura 4.53 é apresentado as falhas de login em um período de 1 hora, já no gráfico das Figura 4.54 e 4.55

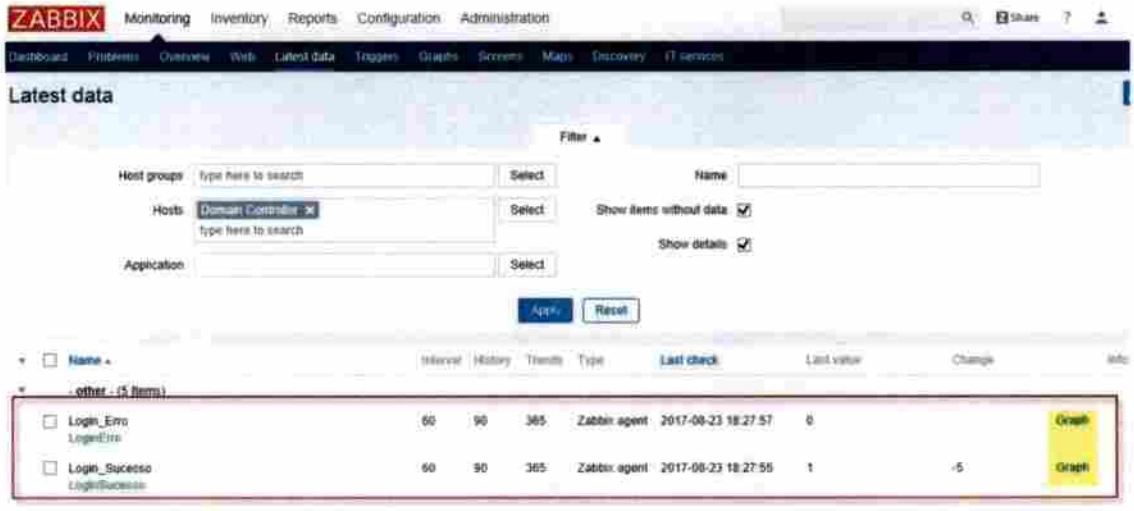
do item "Login_sucesso", é apresentado os dados coletados e armazenados nos períodos de 13 minutos e 1 hora.

Figura 4.50 – Captura de tela do Zabbix, filtro de dados recentes.



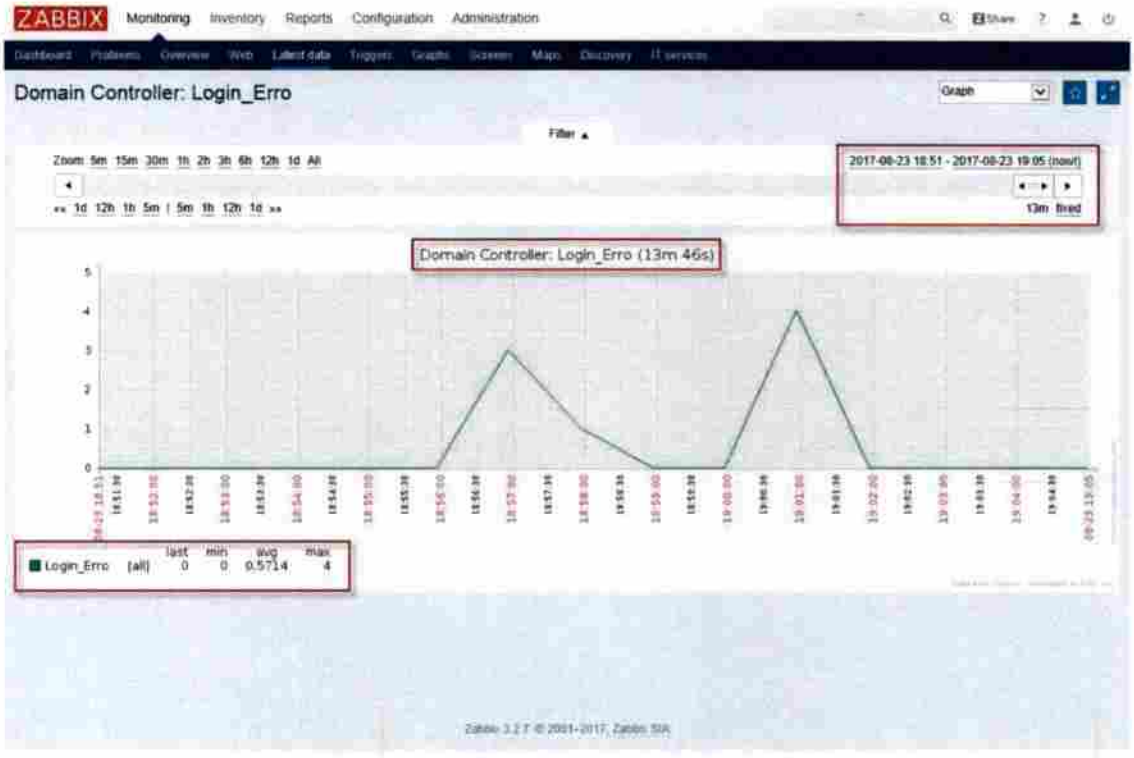
Fonte: própria.

Figura 4.51- Captura de tela do Zabbix: itens do filtro.



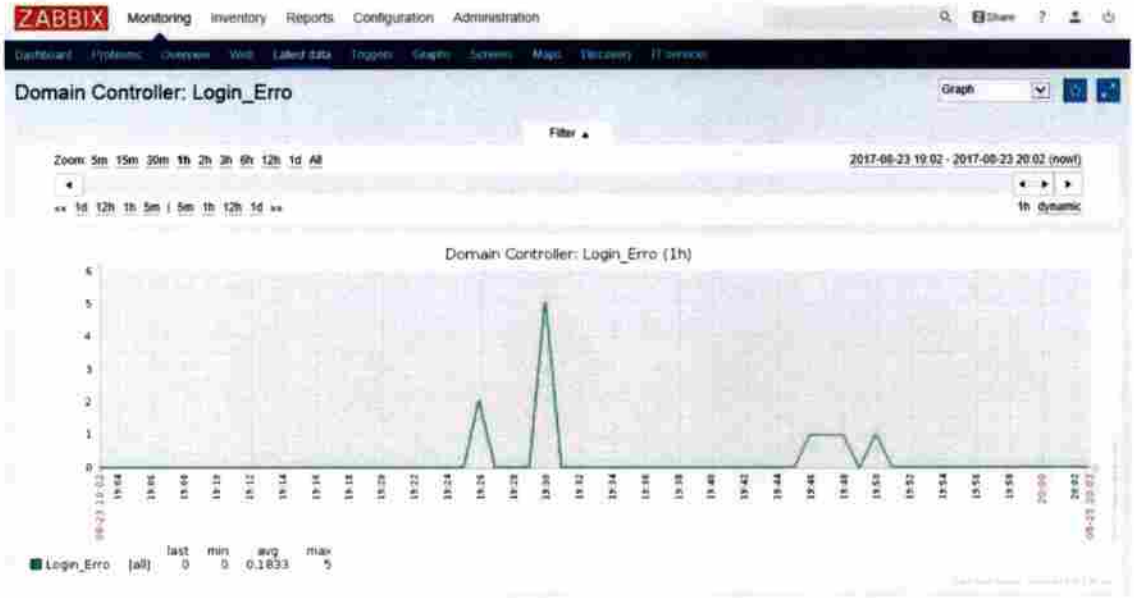
Fonte: própria.

Figura 4.52 - Captura de tela do Zabbix: Gráfico do item "Login_Erro", 13 minutos.



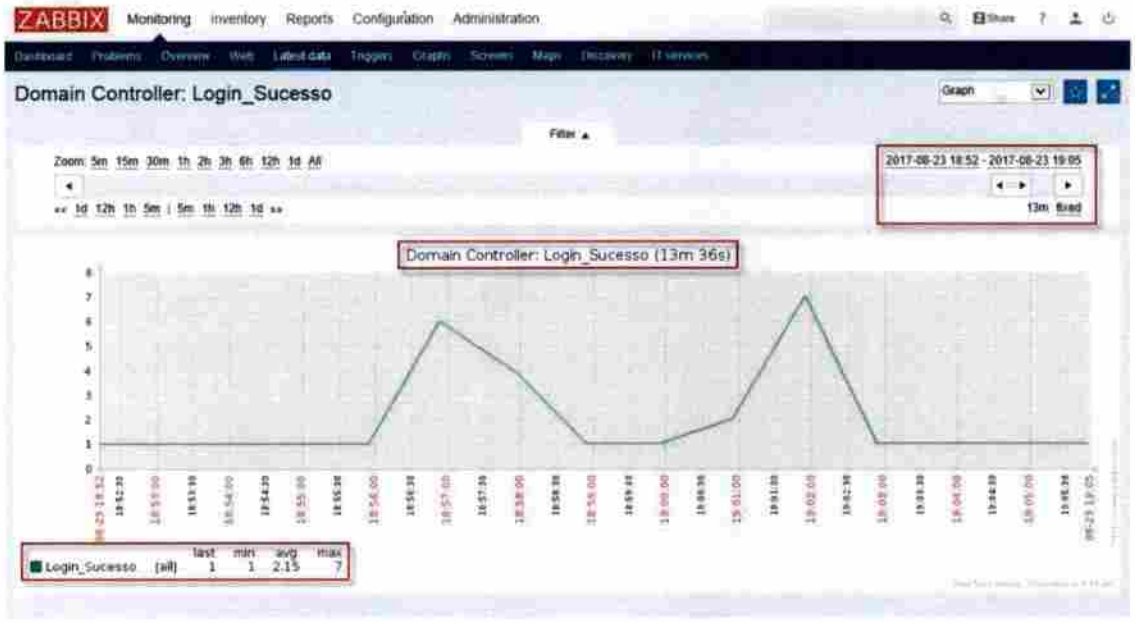
Fonte: própria.

Figura 4.53 - Captura de tela do Zabbix: Gráfico do item "Login_Erro", 1 hora.



Fonte: própria.

Figura 4.54 - Captura de tela do Zabbix: Gráfico do item "Login_Sucesso", 13 minutos.



Fonte: própria.

Figura 4.55 - Captura de tela do Zabbix: Gráfico do item "Login_Sucesso", 1 hora.

Fonte: própria.

Neste capítulo conseguimos construir um ambiente virtual de laboratório, com o Hypervisor VirtualBox, que nos permitiu levantar uma infraestrutura de domínio e de monitoramento básica, com o Microsoft Active Directory e o Zabbix. Para validar e evidenciar que é possível coletar as tentativas de autenticação de usuários e serviços de rede em um controlador de domínio, através da configuração da auditoria, que permitiu o registro no log de segurança, dos identificadores (4624 e 4771) relacionados as tentativas de autenticação, viabilizando assim que os scripts construídos nesse capítulo fossem executados periodicamente através do agente Zabbix, para filtrar e contabilizar o número de tentativas de logon com sucesso ou falha, repassando esses dados ao servidor Zabbix, que os armazena em seu banco de dados, para que o seu componente de interface Web possa gerar os gráficos que foram apresentados aqui. Assim permitir que as equipes de analistas e gestores nas organizações consigam utilizar desses dados na construção de linhas de base, utilizadas para detectar possíveis anomalias na infraestrutura de autenticação e de segurança nas organizações. Além da credibilidade que esses gráficos irão agregar aos relatórios e laudos técnicos do ambiente. No próximo capítulo iremos apresentar as conclusões a respeito do conteúdo construído neste trabalho.

5 - CONCLUSÕES

Através do capítulo 2 (dois) deste trabalho, apresentamos o conteúdo teórico básico para a compreensão dos processos necessários para a realização de autenticação de usuários e serviços em infraestruturas de autenticação baseadas no Microsoft Active Directory. Também fora comentado sobre o protocolo Kerberos e descrito a auditoria em controladores de Domínios da Microsoft, no capítulo quatro habilitamos a auditoria no controlador de domínio. Através do capítulo 3 (três) deste trabalho, fomos capazes de apresentar minimamente o material teórico sobre a estrutura da ferramenta de monitoramento Zabbix, sendo que no capítulo 4 (quatro) também houve algumas referências teóricas e execução do processo de instalação e configuração da ferramenta e seus componentes em um único host. Já no capítulo 4 (quatro) você pode ver na prática como o processo de autenticação realizado e como é simples habilitar nas configurações do controlador de domínio o registro em logs do processo de autenticação, permitindo assim a realização de visualizações e auditoria dos processos. Sendo que só foi possível a execução dos itens práticos desse trabalho graças a construção de um ambiente virtual no capítulo 4 (quatro), onde foi possível simular um processo de autenticação e posteriormente verificar nos logs do controlador de domínio o registro dos ID's responsáveis pela confirmação do sucesso ou falha das requisições de autenticações de usuários e serviços. Com esses ID's sendo registrados em logs, partimos então no mesmo capítulo, para a construção de dois scripts do Microsoft PowerShell, que execute uma varredura nos logs de segurança procurando pelos ID's informados (4624 e 4771) e verifique, se a hora do registro do evento é igual ou superior a menos um minuto da hora atual no controlador de domínio, após esses filtros o script executa a contagem de ocorrências do ID especifico, gerando um resultado final numérico, que será coletado pelo agente do Zabbix que foi previamente instalado e configurado de forma passiva no host, sendo em seguida esse número (dado) transmitido ao servidor de monitoramento para seu armazenamento no banco de dados da ferramenta, esses dados são utilizados pelo componente interface Web na construção de gráficos que utilizamos para geração de uma linha de base e sua análise. Você pode ver que sim, conseguimos mesmo que de forma mínima realizar os objetivos propostos, através do conteúdo apresentado nos capítulos deste trabalho, em especial no capítulo 4, onde foram geradas as evidências necessárias a essa afirmação.

5.1 TRABALHOS FUTUROS

Durante o desenvolvimento deste trabalho, foi visualizado a possibilidade de evolução de vários itens.

Projetar e desenvolver um ambiente de monitoramento com a ferramenta Zabbix, que seja de alta disponibilidade, voltado a atender às necessidades das organizações que precisam cada vez mais registrar a disponibilidade de seus recursos computacionais, buscando no projeto levantar todos os riscos que podem impedir a ferramenta de registrar a disponibilidade ou indisponibilidade dos itens que serão monitorados.

Também podemos trabalhar mais em projetos futuros, as questões relacionadas a uma infraestrutura de autenticação composta por domínios do Microsoft Active Directory, com vários controladores de domínio, buscando monitorar além do processo de autenticação a saúde dos controladores e do AD.

Outro ponto seria a questão de performance dos componentes da ferramenta e dos hosts monitorados, em relação a carga gerada pela própria aplicação Zabbix, além disso precisamos medir a volumetria de dados que os itens monitorados estão utilizando e sua tendência de crescimento, para que possamos utilizar essas informações na análise de possíveis otimizações de ambiente.

REFERÊNCIAS BIBLIOGRÁFICAS

BARTHOLOMEW, D. (2013). *Getting Started with MariaDB.* Birmingham, West Midlands, UK: Packt Publishing Ltd. Retrieved 2017

BOAVIDA, F., BERNARDES, M., & VAPI, P. (2011). *Administração de Redes Informáticas 2ª Edição Actualizada e Aumentada.* Lisboa, Lisboa, Portugal: FCA - Editora de Informatica. Acesso em 2014

DIÓGENES, Y., & MAUSER, D. (2013). *Certificação Security+: da Prática para o Exame SY0-301* (2ª ed.). (A. GARCIA, Ed.) Rio de Janeiro, RJ, Brasil: Novaterra Editora e Distribuidora Ltda. Acesso em 2015

DRILLING, T. (6 de Jun. de 2012). Monitoramento com o Zabbix. *Admin Magazine*, 29. Acesso em 2015

ELLINGWOOD, J. (18 de Jun. de 2015). *How To Set Up a Firewall Using FirewallD on CentOS 7.* Acesso em ago. de 2017, disponível em digitalocean.com: https://www.digitalocean.com/community/tutorials/how-to-set-up-a-firewall-using-firewalld-on-centos-7

FELIPE, B. (26 de maio de 2011). *Como ingressar uma estação a um Domínio do Active Directory.* Acesso em jun. de 2017, disponível em suportederede.wordpress.com: https://suportederede.wordpress.com/2011/05/26/como-ingressar-uma-estacao-a-um-dominio-do-active-directory/

HED HAT. (s.d.). *Enable or Disable SELinux.* Acesso em 2017, disponível em centos.org: https://www.centos.org/docs/5/html/5.1/Deployment_Guide/sec-sel-enable-disable.html

HOLME, D., RUEST, N., RUEST, D., & NORTHRUP, T. (2009). *Kit de Treinamento MCTS (Exame 70-640): configuração do Windows Server 2008 Active Directory.* (E. FURMANKIEWICZ, Trad.) Porto Alegre, RS, Brasil: Bookman. Acesso em 2012

HORST, A. S., PIRES, A. d., & DÉO, A. L. (2015). *De A a ZABBIX* (1ª ed.). (R. PRATES, Ed.) São Paulo, SP, Brasil: Novatec Editora Ltda. Acesso em 2017

LIMA, J. R. (2014). *Monitoramento de Redes com ZABBIX.* (S. M. OLIVEIRA, Ed.) Rio de Janeiro, RJ, Brasil: Brasport.

MACKIN, J. C., & ORION, T. (2016). *Exam Ref 70-412: Configuração dos serviços avançados do Windows Server 2012 R2.* (J. E. TORTELLO, Trad.) Porto Alegrw, RS, Brasil: Bookman. Acesso em 2017

MANZANO, A. L., & MANZANO, M. I. (2014). *TCC - Trabalho de Conclusão de Curso utilizano o Microsoft Word 2013* (1ª ed.). São Paulo, SP, Brasil: Érica. Acesso em 2016

MARIADB Foundation. (2017). Acesso em Jun. de 2017, disponível em mariadb.org: https://mariadb.com/kb/en/mariadb/yum/

MORAES, A. F. (2010). *Segurança em Redes: Fundamentos* (1ª ed.). São Paulo, SP, Brasil: Érica. Acesso em 2015

MOTA FILHO, J. (2012). *Descobrindo o Linux: entenda o sistema operacional GNU/Linux* (3ª ed.). São Paulo, SP, Brasil: Novatec Editora. Acesso em 2016

MOTA, A. P. (5 de mar. de 2012). *Direcionando a saída de um comando no MS-DOS*. Acesso em jul. de 2017, disponível em anapaulamota.wordpress.com: https://anapaulamota.wordpress.com/2012/03/05/direcionando-a-saida-de-um-comando-no-ms-dos/

NAKAMURA, E. T., & GEUS, P. L. (2007). *Segurança de Redes em Ambiente Cooperativos*. São Paulo, SP, Brasil: Novatec Editora Ltda. Acesso em 2013

PAYETTE, B. (2008). *Windows PowerShell em ação*. (F. MAGALHÃES, Trad.) Rio de Janeiro, RJ, Brasil: ALTA BOOKS. Acesso em 2015

RAMOS, D. (14 de fev. de 2015). *Como habilitar a execução de scripts em PowerShell*. Acesso em 2017, disponível em Microsoft Technet: https://social.technet.microsoft.com/wiki/pt-br/contents/articles/29932.como-habilitar-a-execucao-de-scripts-em-powershell.aspx

RYAN, S., & RON, P. (2003). *Aprenda em 24 horas SQL*. (A. B. TAVARES, Trad.) Rio de Janeiro, RJ, Brasil: CAMPUS. Acesso em 2014

STALLINGS, W. (2008). *Criptografia e segurança de redes* (4ª ed.). São Paulo, SP, Brasil: Person Prentice Hall.

STANEK, W. (2009). *Windows Server 2008 Guia Completo*. (T. SOUZA, Trad.) Porto Alegre, RS, Brasil: Bookman. Acesso em jul. de 2011

TANENBAUM, A. S. (2003). *Redes de computadores* (4ª ed.). (V. D. SOUZA, Trad.) Rio de Janeiro, RJ, Brasil: Elsevier.

VELTEM, F. L. (abr. de 2014). *Instalando um Controlador de Domínio Windows Server 2012 r2*. Acesso em jun. de 2017, disponível em social.technet.microsoft.com: https://social.technet.microsoft.com/wiki/pt-br/contents/articles/23481.instalando-um-controlador-de-dominio-windows-server-2012-r2.aspx

VERAS, M. (2011). *Virtualização: Componente Central do Datacenter* (1ª ed.). (S. M. OLIVEIRA, Ed.) Rio de Janeiro, RJ, Brasil: Brasport. Acesso em 2012

ZABBIX SIA. (2017). *Manual do Zabbix*. Acesso em jun. de 2017, disponível em zabbix.com: https://www.zabbix.com/documentation/3.2/pt/manual

ZACKER, C. (2015). *Exam Ref 70-410 : instalação e configuração do Windows Server 2012 R2.* (A. J. SILVA, Trad.) Porto Alegre, RS, Brasil: Bookman. Acesso em 2017

ZÚQUETE, A. (2013). *Seguraça em Redes Informáticas* (4ª ed.). Lisboa, Lisboa, Portugal : FCA - Editora de Informática, Ltda. Acesso em 2015