

# Relatório Técnico de Atividade de Pesquisa

## SPRINT 57 - Atualizar Minhas Informações Pessoais

### OBJETIVO

Descrever o processo de análise e indicar a melhor alternativa para implantação da USER STORY “**Eu como SETIC , preciso que o Sauron informe ao usuário que ele está bloqueado no AD**”.

### JUSTIFICATIVA

Após realização de diversas reuniões com o time da Infra, o time de desenvolvimento identificou que as consultas atualmente utilizadas pela aplicação Sistema de Autenticação do Estado de Rondônia - SAURON, em determinados cenários, estão retornando um valor inesperado, impossibilitando o gerenciamento automatizado do grupo de usuários **desabilitados** do Diretório de Usuários (AD).

### RESULTADOS ESPERADOS

1. Relatório contendo a análise da causa-raiz do problema relacionado ao retorno do valor inesperado.
2. Breve explicação sobre a utilização de Diretórios de Usuários (AD).
3. Análise das propriedades do AD que atendam nossa demanda.
4. Análise da Documentação da Biblioteca Novell.
5. Análise da Documentação da Biblioteca DirectoryServices.

### ENVOLVIDOS

- Gabriel Fernandes (Scrum Master)
- Maria Luiza (Product Owner)
- Guardiões da Galáxia (DEV Team)

### GLOSSÁRIO

- AD - Active Directory - é uma implementação de serviço de diretório no protocolo LDAP.
- LDAP - Lightweight Directory Access Protocol é um protocolo de aplicação de serviços de informação de diretório distribuído sobre uma rede de Protocolo da Internet.
- ADAM - Active Directory Application Mode - uma aplicação que estende as utilizações do LDAP, também chamada de AD LDS.
- NOVELL - empresa de TI que possui uma biblioteca para consumo dos dados do AD via LDAP em C#.

## PREMISSAS

1. O Serviço de Diretório de Usuários (AD), apesar de ser parte da SETIC, é gerenciado pelo time de Infraestrutura de TI.
2. O AD é responsável pelo acesso de todos os usuários que estão na hierarquia da SETIC.
3. Qualquer informação de acesso e usuário deve ser obtida a partir deste Serviço.

## ACTIVE DIRECTORY

### DEFINIÇÃO

O Active Directory (AD) é uma ferramenta de gerenciamento de usuários de rede, denominada serviço de diretório. Um diretório nada mais é do que um banco de dados contendo informações dos usuários de uma organização, tais como nome, login, senha, cargo, perfil e etc.

O AD é implementado em protocolo LDAP (Lightweight Directory Access Protocol), que, traduzido ao pé da letra, significa: Protocolo Leve de Acesso a Diretório. Trata-se de um protocolo livre que é conhecido como o padrão do mercado para gerenciamento de informações de diretório distribuído sobre uma rede de Protocolo da Internet (IP).

Através da implementação de serviço LDAP, o Active Directory permite o uso de um único diretório para controle de acesso a todos sistemas e serviços dentro de uma rede corporativa. Isso significa que o colaborador de uma empresa não precisa criar um usuário e senha para cada sistema que tiver acesso, e sim utilizar seu usuário e senhas únicos(as).

### PROPRIEDADES RELEVANTES

Para atender a demanda, serão analisadas as propriedades relacionadas com a habilitação/deshabilitação da conta do usuário do AD.

- ms-DS-User-Account-Disabled
  - Descrição: Indica se uma conta está desativada ou ativada.
  - Nome LDAP: msDS-UserAccountDisabled
  - Retorno: Booleano
    - true - Desativado
    - false - Ativado
  - Implementação - Somente ADAM
- User-Account-Control
  - Descrição: Sinalizadores que controlam o comportamento da conta do usuário.
  - Nome LDAP: userAccountControl
  - Retorno: 4bytes (HEX)
    - 0x00000002 - ADS\_UF\_ACCOUNTDISABLE - conta desativada.
    - 0x00000010 - ADS\_UF\_LOCKOUT - conta bloqueada
    - 0x00000200 - ADS\_UF\_NORMAL\_ACCOUNT - conta normal
    - 0x00800000 - ADS\_UF\_PASSWORD\_EXPIRED - senha expirada

- Implementação - Windows 2000 , 2003 (R2), 2008 (R2) e 2012

## BIBLIOTECAS AUXILIARES

### NOVELL

A propriedade “user-AccountControl” é suportada pela biblioteca NOVELL ( <https://www.novell.com/documentation/idm35drivers/ad/data/bp8d4f4.html> ), não sendo necessárias alterações na estrutura atual de código. Quanto a propriedade “ms-Ds-UserAccountDisabled”, a documentação da Biblioteca orienta o pareamento da informação fornecida pela primeira propriedade para obter o valor desejado ( <https://www.novell.com/coololutions/trench/8558.html> )

### DIRECTORY SERVICES

A propriedade “user-AccountControl” é suportada pela biblioteca Directory Services ( <https://support.microsoft.com/pt-br/help/305144/how-to-use-useraccountcontrol-to-manipulate-user-account-properties> ) não sendo necessárias alterações na estrutura atual de código.

## PROPOSTAS

A seguir são descritas duas abordagens possíveis para a implantação, sendo destacadas quais as ações associadas são necessárias para a implantação da User Story, seguidas de um estudo da complexidade envolvida com o processo de desenvolvimento de cada uma dessas ações. Os valores de complexidade foram atribuídos após reunião entre os participantes.

### 1.UTILIZAÇÃO DO SERVIÇO ADAM

- AÇÕES ASSOCIADAS
  - Alinhamento com a equipe de Infraestrutura de TI (1 Ponto - CADA)
  - Análise da Viabilidade de Implantação por parte da Infra (2 Pontos - INFRA)
  - Instalação, Configuração e Disponibilização (se viável) (3 Pontos - INFRA)
  - Pareamento no Código (1 Ponto - DEV)
  - Testes realizados (1 Ponto - DEV)
- COMPLEXIDADE - constante para cada questão adicionada.  
Considerando  $C(n) = (\sum P\_INFRA + \sum P\_DEV) = 9$  pontos de complexidade, sendo 6 pontos para a equipe de Infraestrutura de TI e 3 pontos para a equipe DEV.

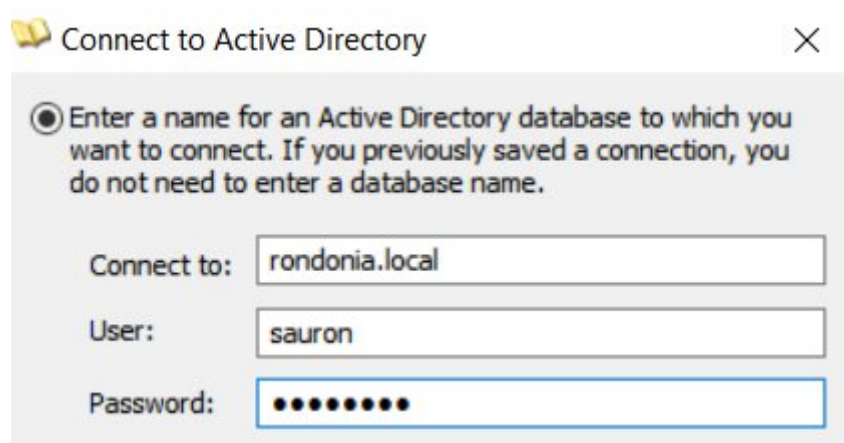
### 2.UTILIZAÇÃO DA PROPRIEDADE USER-ACCOUNTCONTROL

- AÇÕES ASSOCIADAS
  - Alinhamento com a equipe de Infraestrutura de TI (1 Ponto - CADA)
  - Identificação dos Cenários para Calculo Binário ( 1 Ponto - CADA)
  - Pareamento no Código (1 Ponto - DEV)
  - Calculo do valor pareado de acordo com cenários (3 Pontos - DEV)
  - Testes realizados (1 Ponto - DEV)

- COMPLEXIDADE - constante para cada questão adicionada.  
Considerando  $C(n) = (\sum P\_INFRA + \sum P\_DEV) = 9$  pontos de complexidade, sendo 2 pontos para a equipe de Infraestrutura de TI e 7 pontos para a equipe DEV.

## EXEMPLO

Para exemplificar o calculo binário da propriedade “**user-AccountControl**”, realizaremos o calculo para dois usuários do nosso AD, comparando os resultados com a tabela em anexo, no fim deste documento. Para este experimento utilizaremos a aplicação Microsoft ADEplorer com as credenciais da aplicação Sauron, como demonstrado a seguir:



Connect to Active Directory

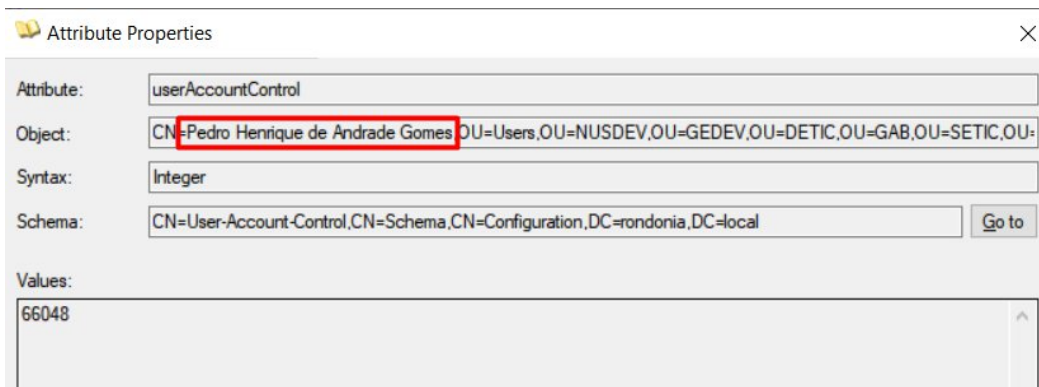
Enter a name for an Active Directory database to which you want to connect. If you previously saved a connection, you do not need to enter a database name.

Connect to: rondonia.local

User: sauron

Password: ●●●●●●●●

- EXEMPLO 1
  - Usuário: Pedro Henrique de Andrade Gomes
  - userAccountControl: 66048



Attribute Properties

Attribute: userAccountControl

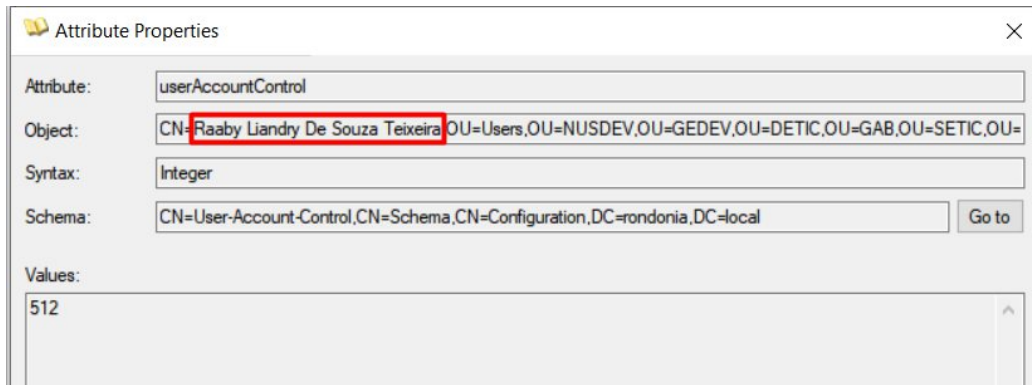
Object: CN=Pedro Henrique de Andrade Gomes,OU=Users,OU=NUSDEV,OU=GEDEV,OU=DETIC,OU=GAB,OU=SETIC,OU=...

Syntax: Integer

Schema: CN=User-Account-Control,CN=Schema,CN=Configuration,DC=rondonia,DC=local [Go to](#)

Values: 66048

- EXEMPLO 2
  - Usuário: Raaby Liandry de Souza Teixeira
  - userAccountControl: 512



Para o Exemplo 1, onde o valor obtido foi 66048, ao calcularmos as propriedades do usuário a partir da tabela presente no anexo 1, temos:

$$\text{NORMAL\_ACCOUNT (512)} + \text{DONT\_EXPIRE\_PASSWORD (65536)} = 66048$$

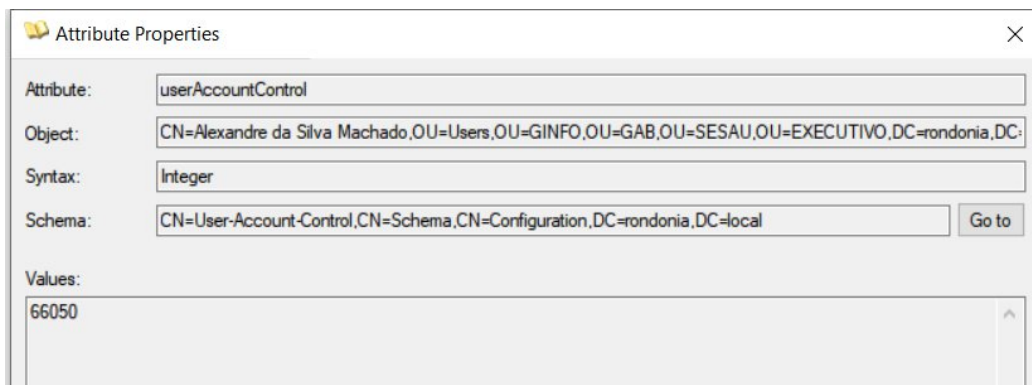
Logo, o usuário possui uma conta normal, com a opção de não expiração de senha ativada.

Para o exemplo 2, onde o valor obtido é 512 temos:

$$\text{NORMAL\_ACCOUNT (512)}$$

Sabendo que a propriedade `ACCOUNTDISABLE (2)` logo, ao subtrair 2 da propriedade se subtrairmos apenas valores que são potências de 2, do maior para o menor possível e chegarmos no valor 0, então o usuário possui uma conta desativada.

Um exemplo para consolidação é o exemplo a seguir:



Para o usuário em questão temos o valor 66050.

$$1^{\circ} \text{ passo - subtraímos } 2^{16} \text{ ( DONT\_EXPIRE\_PASSWORD (65536) ) } = 514$$

$$2^{\circ} \text{ passo - subtraímos } 2^9 \text{ ( NORMAL\_ACCOUNT (512) ) } = 2$$

$$3^{\circ} \text{ passo - subtraímos } 2^1 \text{ ( ACCOUNTDISABLE (2) ) } = 0$$

Logo, temos certeza que a conta do usuário está **desabilitada**.

## RESULTADOS

Na Tabela 1 é apresentado um comparativo entre as alternativas propostas para a resolução da User Story em questão. Para cada opção é considerado os pontos de

complexidade para o time de desenvolvedores e para o time de infraestrutura de TI. São levados em conta quatro diferentes aspectos descritos a seguir:

- **Complexidade Técnica** - dificuldade para entendimento, elucidação e implantação da solução proposta em linhas de código.
- **Configuração** - dificuldade de implantação da solução por parte da equipe de infraestrutura de TI.
- **Sustentabilidade** - dificuldade de garantia de qualidade e manutenção da solução como um todo.
- **Responsabilidade** - quantidade de responsabilidade herdada pela aplicação (Sauron).

Tabela 1. Comparativo da complexidade ( C(n) ), pontos fortes e fracos das opções analisadas.

OP	C(n)	PONTOS FORTES	PONTOS FRACOS
1	DEV - 3 INFRA - 6	<ul style="list-style-type: none"> <li>• complexidade técnica (-)</li> <li>• sustentabilidade (+)</li> <li>• responsabilidade (-)</li> </ul>	<ul style="list-style-type: none"> <li>• configuração (+)</li> </ul>
2	DEV - 7 INFRA - 2	<ul style="list-style-type: none"> <li>• configuração (-)</li> </ul>	<ul style="list-style-type: none"> <li>• complexidade técnica (+)</li> <li>• sustentabilidade (-)</li> <li>• responsabilidade (+)</li> </ul>

## CONCLUSÃO

Após análise da documentação das bibliotecas e serviços, foi identificado que a propriedade “ms-DS-User-Account-Disabled “ não retorna nenhum valor pois necessita da ativação do serviço ADAM, atualmente indisponível. Será verificado junto a equipe de Infraestrutura de TI a viabilidade da ativação deste serviço a partir da disponibilização do AD LDM (ADAM) e, caso negado, faremos o pareamento da propriedade “User-Account-Control”.

## REFERÊNCIAS

- PORTAL GSTI - <https://www.portalgsti.com.br/active-directory/sobre/>
- ms-UserAccountControl - <https://support.microsoft.com/pt-br/help/305144/how-to-use-useraccountcontrol-to-manipulate-user-account-properties>
- ADAM - <https://www.microsoft.com/pt-br/download/details.aspx?id=4201>
- Exemplo utilização sem ADAM - [https://community.idera.com/database-tools/powershell/ask\\_the\\_experts/f/active\\_directory\\_powershell\\_remoting-9/3565/how-do-i-display-the-msds-useraccountdisabled-attribute](https://community.idera.com/database-tools/powershell/ask_the_experts/f/active_directory_powershell_remoting-9/3565/how-do-i-display-the-msds-useraccountdisabled-attribute)
- Calculo ms-UserAccountControl - <https://social.technet.microsoft.com/Forums/ie/en-US/7ff0fb2f-0cd1-44a9-b172-7abd196ee617/account-disabled-attribute-question?forum=winserverDS>

## APÊNDICE 1 - TABELA DE CONVERSÃO DA PROPRIEDADE “USER-ACCOUNTCONTROL”

Tabela 1. Relação dos Valores em HEX e Decimal

<b>UserAccountControl Flag</b>	<b>HEX Value</b>	<b>Decimal Value</b>
SCRIPT (Running the logon script)	0x0001	1
ACCOUNTDISABLE (The account is disabled)	0x0002	2
HOMEDIR_REQUIRED (The home folder is required)	0x0008	8
LOCKOUT (The account is locked)	0x0010	16
PASSWD_NOTREQD (No password is required)	0x0020	32
PASSWD_CANT_CHANGE (Prevent user from changing password)	0x0040	64
ENCRYPTED_TEXT_PWD_ALLOWED (Store password using reversible encryption)	0x0080	128
TEMP_DUPLICATE_ACCOUNT (An account of a user, whose primary account is in another domain)	0x0100	256
NORMAL_ACCOUNT (A default account, a typical active account)	0x0200	512
INTERDOMAIN_TRUST_ACCOUNT	0x0800	2048
WORKSTATION_TRUST_ACCOUNT	0x1000	4096
SERVER_TRUST_ACCOUNT	0x2000	8192
DONT_EXPIRE_PASSWORD (user accounts with passwords that don't expire)	0x10000	65536
MNS_LOGON_ACCOUNT	0x20000	131072
SMARTCARD_REQUIRED (To log on to the network, the user needs a smart card)	0x40000	262144
TRUSTED_FOR_DELEGATION	0x80000	524288
NOT_DELEGATED	0x100000	1048576
USE_DES_KEY_ONLY	0x200000	2097152

---

DONT_REQ_PREAUTH (Kerberos pre-authentication is not required)	0x400000	4194304
PASSWORD_EXPIRED (The user password has expired)	0x800000	8388608
TRUSTED_TO_AUTH_FOR_DELEGATION	0x1000000	16777216
PARTIAL_SECRETS_ACCOUNT	0x04000000	67108864

---