∏ NetApp

Windows AD サーバ用の AWS セキュリティグループの設定
Cloud Manager

Tom Onacki
April 24, 2021

目次

Windows AD サーバ用の AWS セキュリティグループの設定

クラウドボリュームで Windows Active Directory （ AD ）サーバを使用する場合は、AWS セキュリティグループの設定に関するガイダンスを確認しておく必要があります。この設定により、クラウドボリュームが AD に正しく統合されます。

デフォルトでは、 EC2 Windows インスタンスに適用されている AWS セキュリティグループには、 RDP 以外のプロトコルのインバウンドルールは含まれていません。Cloud Volumes Service からのインバウンド通信を有効にするには、各 Windows AD インスタンスに接続されているセキュリティグループにルールを追加する必要があります。必要なポートは次のとおりです。

サービス	ポート	プロトコル
AD Web サービス	9389	TCP
DNS	53	TCP
DNS	53	UDP
ICMPv4	該当なし	エコー応答
Kerberos	464	TCP
Kerberos	464	UDP
Kerberos	88	TCP
Kerberos	88	UDP
LDAP	389	TCP
LDAP	389	UDP
LDAP	3268	TCP
NetBIOS 名	138	UDP
SAM/LSA	445	TCP
SAM/LSA	445	UDP
セキュアな LDAP	636	TCP
セキュアな LDAP	3269	TCP
W32 時間	123	UDP

AWS EC2 インスタンスに AD インストールドメインコントローラとメンバーサーバを導入して管理する場合は、 Cloud Volumes Service のトラフィックを許可するセキュリティグループのルールがいくつか必要になります。以下は、 AWS CloudFormation テンプレートの一部として AD アプリケーションにこれらのルールを実装する方法の例です。

```
{
    "AWSTemplateFormatVersion" : "2010-09-09",
    "Description" : "Security Group for AD",
    "Parameters" :
```

```json
    {
        "VPC" :
        {
            "Type" : "AWS::EC2::VPC::Id",
            "Description" : "VPC where the Security Group will belong:"
        },
        "Name" :
        {
            "Type" : "String",
            "Description" : "Name Tag of the Security Group:"
        },
        "Description" :
        {
            "Type" : "String",
            "Description" : "Description Tag of the Security Group:",
            "Default" : "Security Group for Active Directory for CVS "
        },
        "CIDRrangeforTCPandUDP" :
        {
            "Type" : "String",
            "Description" : "CIDR Range for the UDP ports
445,138,464,389,53,123 and for the TCP ports
464,339,3389,3268,88,636,9389,445 and 0-65535: *CIDR range format:
10.0.0.0/24"
        }
    },
    "Resources" :
    {
        "ADSGWest" :
        {
            "Type" : "AWS::EC2::SecurityGroup",
            "Properties" :
            {
                "GroupDescription" : {"Ref" : "Description"},
                "VpcId" : { "Ref" : "VPC" },
                "SecurityGroupIngress" : [
                    {
                        "IpProtocol" : "udp",
                        "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                        "FromPort" : "445",
                        "ToPort" : "445"
                    },
                    {
                        "IpProtocol" : "udp",
                        "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                        "FromPort" : "138",
```

```json
                "ToPort" : "138"
            },
            {

                "IpProtocol" : "udp",
                "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                "FromPort" : "464",
                "ToPort" : "464"
            },
            {

                "IpProtocol" : "tcp",
                "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                "FromPort" : "464",
                "ToPort" : "464"
            },
            {

                "IpProtocol" : "udp",
                "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                "FromPort" : "389",
                "ToPort" : "389"
            },
            {

                "IpProtocol" : "udp",
                "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                "FromPort" : "53",
                "ToPort" : "53"
            },
            {
                "IpProtocol" : "tcp",
                "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                "FromPort" : "339",
                "ToPort" : "339"
            },
            {
                "IpProtocol" : "udp",
                "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                "FromPort" : "123",
                "ToPort" : "123"
            },
            {
                "IpProtocol" : "tcp",
                "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                "FromPort" : "3389",
                "ToPort" : "3389"
            },
            {
                "IpProtocol" : "tcp",
```

```json
                    "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                    "FromPort" : "3268",
                    "ToPort" : "3268"
                },
                {

                    "IpProtocol" : "tcp",
                    "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                    "FromPort" : "88",
                    "ToPort" : "88"
                },
                {

                    "IpProtocol" : "tcp",
                    "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                    "FromPort" : "636",
                    "ToPort" : "636"
                },
                {

                    "IpProtocol" : "tcp",
                    "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                    "FromPort" : "3269",
                    "ToPort" : "3269"
                },
                {

                    "IpProtocol" : "tcp",
                    "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                    "FromPort" : "53",
                    "ToPort" : "53"
                },
                {

                    "IpProtocol" : "tcp",
                    "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                    "FromPort" : "0",
                    "ToPort" : "65535"
                },
                {

                    "IpProtocol" : "tcp",
                    "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                    "FromPort" : "9389",
                    "ToPort" : "9389"
                },
                {

                    "IpProtocol" : "tcp",
                    "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                    "FromPort" : "445",
                    "ToPort" : "445"
                }
```

```
                ]
            }
        }
    },
    "Outputs" :
    {
        "SecurityGroupID" :
        {
            "Description" : "Security Group ID",
            "Value" : { "Ref" : "ADSGWest" }
        }
    }
}
```