



AWS security group settings for Windows AD servers

Cloud Manager

Tom Onacki
June 09, 2021

This PDF was generated from https://docs.netapp.com/us-en/occm/reference_security_groups_windows_ad_servers.html on September 09, 2021. Always check docs.netapp.com for the latest.

Table of Contents

AWS security group settings for Windows AD servers..... 1

AWS security group settings for Windows AD servers

If you use Windows Active Directory (AD) servers with cloud volumes, you should familiarize yourself with the guidance on AWS security group settings. The settings enable cloud volumes to integrate with AD correctly.

By default, the AWS security group applied to an EC2 Windows instance does not contain inbound rules for any protocol except RDP. You must add rules to the security groups that are attached to each Windows AD instance to enable inbound communication from Cloud Volumes Service. The required ports are as follows:

| Service | Port | Protocol |
|-----------------|------|------------|
| AD Web Services | 9389 | TCP |
| DNS | 53 | TCP |
| DNS | 53 | UDP |
| ICMPv4 | N/A | Echo Reply |
| Kerberos | 464 | TCP |
| Kerberos | 464 | UDP |
| Kerberos | 88 | TCP |
| Kerberos | 88 | UDP |
| LDAP | 389 | TCP |
| LDAP | 389 | UDP |
| LDAP | 3268 | TCP |
| NetBIOS name | 138 | UDP |
| SAM/LSA | 445 | TCP |
| SAM/LSA | 445 | UDP |
| Secure LDAP | 636 | TCP |
| Secure LDAP | 3269 | TCP |
| w32time | 123 | UDP |

If you are deploying and managing your AD installation domain controllers and member servers on an AWS EC2 instance, you will require several security group rules to allow traffic for the Cloud Volumes Service. Below is an example of how to implement these rules for AD applications as part of the AWS CloudFormation template.

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

```

"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",
          "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",
  "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" }  
    }  
  }  
}
```

Copyright Information

Copyright © 2021 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system-without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark Information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.