

Management Center for Cisco Security Agents High Availability White Paper

This whitepaper discusses the Management Center for Cisco Security Agents (CSA MC) High Availability (HA) solution.

The CSA MC high availability solution uses a primary and secondary CSA MC to provide agents with maximum access to a Management Center. Generally, Cisco Security Agents (agents) communicate with CSA MC when it is in the “reachable” system state. When the CSA MC is not reachable, the agents will not send events, receive software upgrades, or receive policy updates. The CSA MC may not be reachable for many reasons including scheduled upgrades, network connectivity issues, the CSA MC service has been stopped, or there has been a server outage.

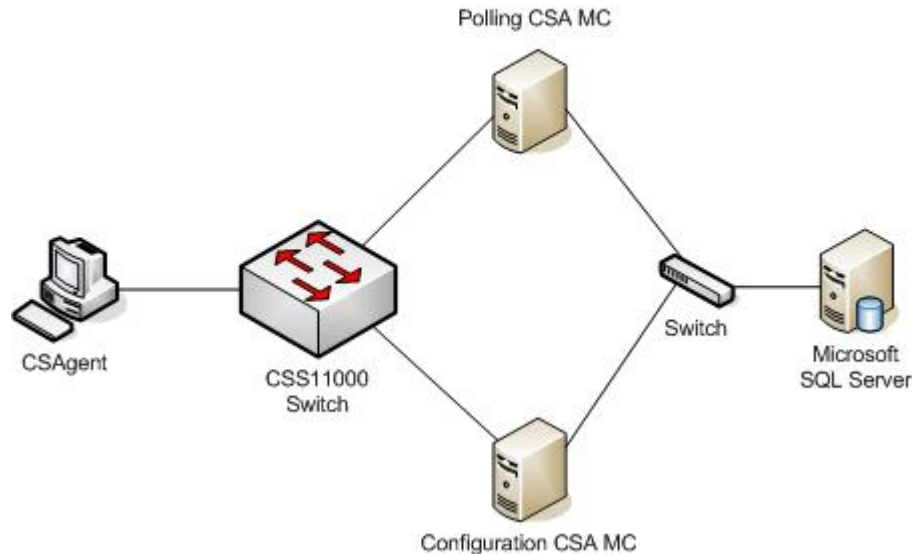
The current method of recovering from a down CSA MC is to create a secondary CSA MC, keeping it offline, with same name and IP address as primary CSA MC, copy all SSL certificates from the primary to the secondary CSA MC, export all data from the primary CSA MC, import the data to the secondary CSA MC, shutdown the primary CSA MC and start the secondary CSA MC. This is a very time consuming process during which agents have no access to a CSA MC.

With the CSA MC HA solution, the secondary CSA MC is ready to take over for the primary CSA MC as soon as it is needed. The primary CSA MC does not need to have network connectivity in order for this switchover to occur. When the primary CSA MC is ready to resume its role, it connects to the network and it begins to act as the primary once again.

Management Center for Cisco Security Agent High Availability Solution

The recommended Management Center for Cisco Security Agent High Availability Solution uses a Cisco 11000 Series Content Service Switch (CSS), configured with a content rule, to NAT (Network Address Translation) and a 3-Tier CSA MC configuration. The 3-Tier CSA MC configuration is made up of a polling CSA MC, a configuration CSA MC, and a remote database to which both CSA MCs are connected. The polling CSA MC acts as the primary Management Center and the configuration CSA MC acts as the secondary Management Center. See Figure 1.

Figure 1. Management Center for Cisco Security Agents High Availability Topology
 Management Center for Cisco Security Agent High Availability Topology



The software requirements for this solution are Web Network Services (WebNS) Software Release 3.x or later for the CSS, Microsoft SQL Server 2000 or 2005 for the remote database server, and Cisco Security Agent Version 6.0 or later for CSA MC.

The CSS is configured with a content rule to NAT the polling CSA MC. When the polling CSA MC is unavailable, the CSS sends all traffic for the polling CSA MC to the configuration CSA MC. Because the CSS is NATing, the agents sending the traffic are unaware and unaffected by the traffic being sent to the configuration CSA MC. When the polling CSA MC is available, all traffic is sent to it and not the configuration CSA MC.

The 3-Tier CSA MC configuration uses two CSA MC servers that are connected to the same remote Microsoft SQL database. One CSA MC is the polling server which manages agent events, polling, software upgrades, and policy updates. The configuration CSA MC is used to create policies and agent kits and configure the CSA MC.

Configure the polling CSA MC first and connect it to the remote Microsoft SQL database. Configure the configuration CSA MC second and connect it to the same remote Microsoft SQL database. Once both CSA MCs are connected to the database, the first CSA MC is automatically designated the polling CSA MC and the second CSA MC is automatically designated the configuration CSA MC. All agent and CSA MC data is stored in the remote database. All SSL information for the CSA MC and agent kits are generated using the hostname of the polling CSA MC.

The CSS configuration contains two services (services on the CSS are the CSA MC servers), one content rule, and one source group. The content rule is configured with a Virtual IP Address (VIP) that contains the polling CSA MC as a service and the configuration CSA MC as polling CSA MC's primarySorryServer. The primarySorryServer is a backup service (server) that is used when the primary service is down or unavailable. All traffic destined for the VIP will be NATed to the service on the VIP, in this case, the polling CSA MC. If the content rule's primary service (the polling CSA MC) is down or unavailable, the primarySorryServer is used. When the primary service is up and available again, all traffic is sent to the primary service. The CSS configuration also contains circuit addresses. The circuit addresses are network subnets for the agents and the CSA MCs. The circuit addresses are needed for the CSS to communicate and NAT with the different subnets. The agent traffic to the CSA MC may be

NATed with the source address of the CSS circuit address that the CSAgents use based on their subnet. A source group is also configured on the CSS. A content rule will NAT all traffic destined to its services (the CSA MCs). A source group NATs all traffic originated from the services configured on it. A source group also has a VIP, which is the address used its NATing. The source group will have the CSA MCs configured as services. The CSA MCs originate traffic to the agents for polling hints. A source group NATs the traffic from the CSA MC to the agents with the source group VIP and not the CSA MC address. Without a source group the polling hints will have a source address of the CSA MC, however the agents believe the CSA MC has an address of the content rule VIP. For this reason, the VIP on the source group must match the VIP of the content rule.

See the [Cisco CSS Configuration Example on page 4](#) for more configuration information.

Part of the requirements for the CSS configuration is to have DNS server entries for the content rule on the CSS. The reason for this is that the CSAgents send traffic to the CSA MC by hostname, not IP address. The CSAgents will perform a CSA MC hostname lookup (via DNS, local hosts table, etc.). The CSA MC lookup will resolve to the content rule on the CSS. The agent will send all traffic to the CSS which will NAT the traffic to the CSA MC.

When the polling CSA MC is down or unavailable, all traffic destined to the VIP will be sent to the configuration CSA MC. Because the traffic is NATed and the agent and CSA MC data is stored in the remote database, the agents do not know they are communicating with the configuration CSA MC. The VIP on the CSS appears to be the polling CSA MC to the CSAgents because of the DNS/hostname lookups return the polling CSA MC hostname with the CSS VIP address. The CSAgent traffic is sent to the VIP address which is then NATed to the appropriate CSA MC. The CSA MCs communicate with the CSAgents only through the CSS.

To have a complete high availability solution, it is recommended to have a Microsoft SQL Server Failover Cluster for the remote database. Go to <http://support.microsoft.com> for information about SQL Server Failover Clusters.

How Management Center for Cisco Security Agent HA Solution Works with MC Fail-Over

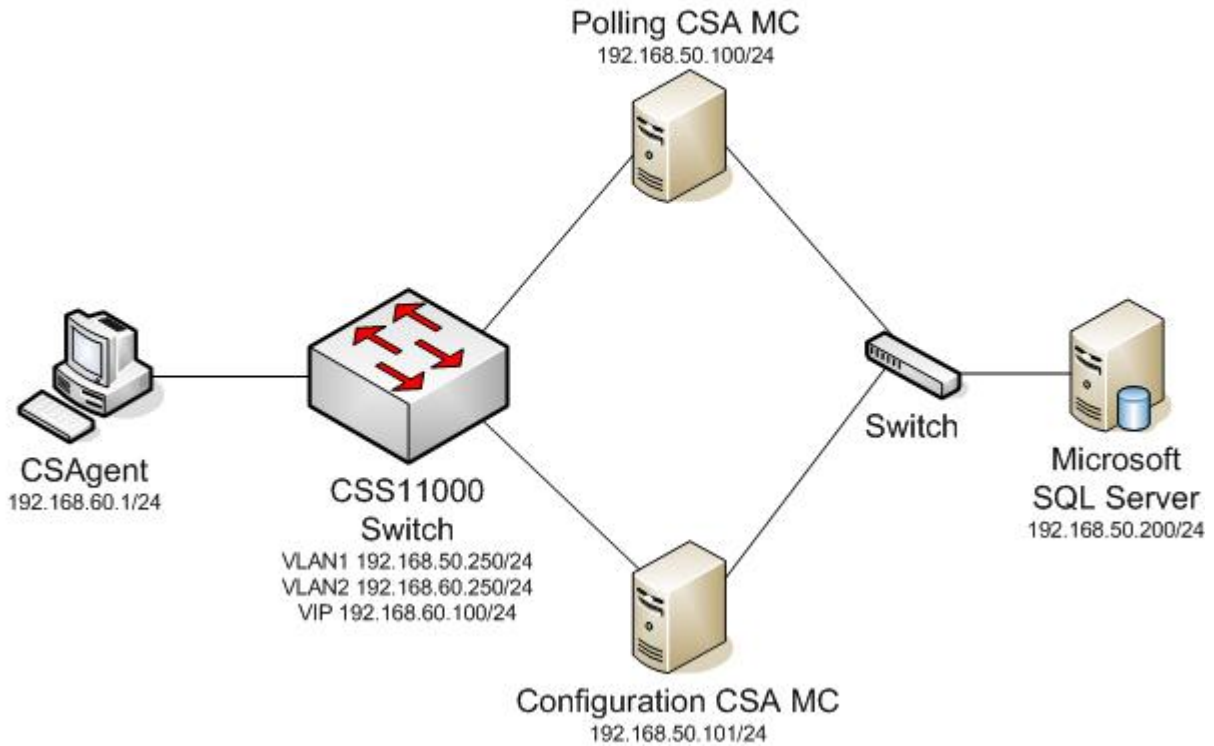
The CSS has the CSA MCs configured as services. It uses a content rule for the polling CSA MC. The configuration CSA MC is configured as the primarySorryServer (backup server) for the polling CSA MC. The CSS will change the polling CSA MC state to Down when it is unreachable or if the keepalive configured on the polling CSA MC service detects a failure. It is recommended to have a service keepalive type of TCP for the CSA MC services. A keepalive type of TCP will detect when there is a failure to connect to the TCP port configured on the service (the default is port 80, which is the default CSA MC web server port). A keepalive failure or network reachability failure or configuration change of the polling CSA MC service state to suspend will cause the CSS to send traffic to the primarySorryServer, the configuration CSA MC. When the polling CSA MC is in the Alive/Up state, all traffic will be sent to it. The CSS will not send traffic to a service in the Down or Suspend state. If both CSA MC servers are down, all traffic destined for the CSA MC will fail.

How to upgrade CSA MC software version with CSA MC HA Solution

To upgrade the CSA MC software version with a CSA MC HA configuration, both polling and configuration CSA MCs must be unreachable by the agents. Because the CSA MC data is stored in the remote database, many problems will arise when the agents communicate with a CSA MC that is running a version of software that is different than the data stored in the remote database. Only after both CSA MCs are upgraded to the newer version, the CSAgents should be made reachable to the CSA MCs.

WARNING: The polling and configuration CSA MCs must be unreachable by the agents during the CSA MC software upgrade process. Both the polling and configuration CSA MCs must be upgraded to the same version of CSA software before either is reachable. You risk corrupting the CSA MC and agent data in the remote database if either CSA MC is reachable to the agents before both are upgraded.

Figure 2. Management Center for Cisco Security Agent High Availability Topology with Addressing
**Management Center for Cisco Security Agent High Availability Topology
 With Network Addressing**



Cisco CSS Configuration Example

```
conf i gur e

! ***** I NTERFACE *****
i nter face e1
  description "polling CSA MC Interface"
  ! vl an 1 not di spl ayed because it is defaul t vl an

i nter face e2
  description "confi gur ation CSA MC Interface"
  ! vl an 1 not di spl ayed because it is defaul t vl an

i nter face e5
  descri ption "CSAgent Interface"
  bri dge vl an 2

i nter face e6
  descri ption "CSAgent Interface"
  bri dge vl an 2

i nter face e7
```

```

description "CSAgent Interface"
bridge vlan 2

interface e8
description "CSAgent Interface"
bridge vlan 2

! ***** CIRCUIT *****
circuit VLAN1
description "CSA MC VLAN"

ip address 192.168.50.250 255.255.255.0

circuit VLAN2
description "CSAgent VLAN"

ip address 192.168.60.250 255.255.255.0

! ***** SERVICE *****
service pollingM
ip address 192.168.50.100
keepalive type tcp
keepalive retryperiod 2
keepalive maxfailure 1
keepalive frequency 2
active

service configM
ip address 192.168.50.101
keepalive type tcp
keepalive retryperiod 2
keepalive maxfailure 1
keepalive frequency 2
active

! ***** OWNER *****
owner csa

content haM
vip address 192.168.60.100
add service pollingM
primarySorryServer configM
active

! ***** OWNER *****
group csa

vip address 192.168.60.100
! NAT traffic originated from the following services
add service pollingM
add service configM
active

```

Related Documentation

Documentation for a 3-Tier CSAMC configuration:

http://www.cisco.com/en/US/docs/security/csa/csa60/install_guide/Installing_CSAMC.html#wp982988

Documentation for a CSAMC with remote database:

http://www.cisco.com/en/US/docs/security/csa/csa60/install_guide/Installing_CSAMC.html#wp978017

Documentation for a CSS with primarySorryServer configuration:

http://www.cisco.com/en/US/products/hw/contnetw/ps789/products_configuration_example09186a0080093de8.shtml

Documentation for CSS Administration:

http://www.cisco.com/en/US/docs/app_ntwk_services/data_center_app_services/css1150series/v8.20/configuration/administration/guide/admgd.html

Documentation for a CSS content load-balancing configuration:

http://www.cisco.com/en/US/docs/app_ntwk_services/data_center_app_services/css1150series/v8.20/configuration/content_lb/guide/cntlbgd.html

Documentation for CSS source groups configuration:

http://www.cisco.com/en/US/docs/app_ntwk_services/data_center_app_services/css1100series/v6.10/configuration/basic/guide/SGACLEQL.html.

Documentation for Microsoft SQL Server 2005 Failover Clustering:

<http://www.microsoft.com/downloads/details.aspx?FamilyID=818234dc-a17b-4f09-b282-c6830fead499&displaylang=en#Instructions>

CCDE, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0812R)