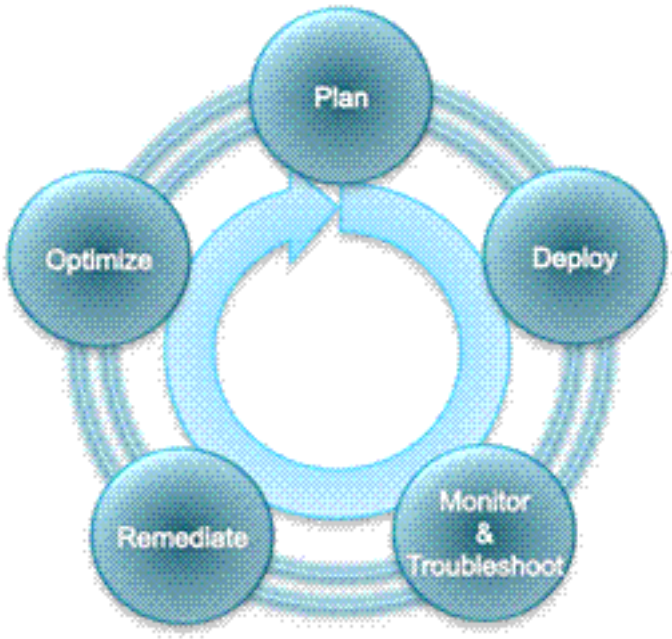
Guia de distribuição da prima NC 1.1 de Cisco

Índice

Introdução

O Cisco Prime Network Control System (NCS) é a próxima geração de plataforma do gerenciamento de rede da Cisco para o gerenciamento de acesso com ou sem fio.



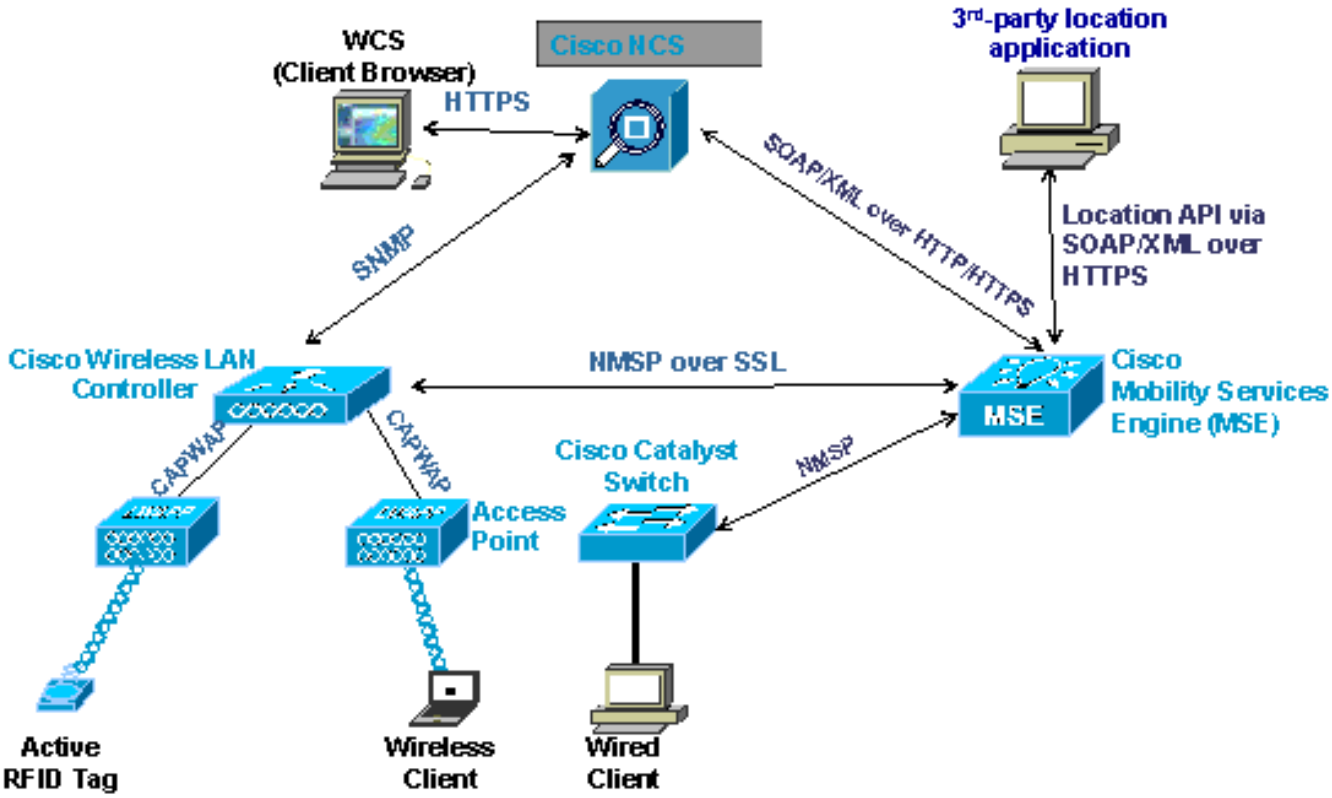
Gerenciamento do ciclo de vida WLAN: O Gerenciamento detalhado do ciclo de vida WLAN inclui uma gama completa de planeamento, desenvolvimento, monitoração e Troubleshooting, remediação e otimização.

- Planejar — O planeamento incorporado e as ferramentas de projeto simplificam a definição da colocação e da cobertura do Access point. Adicionalmente, a informação das ferramentas da terceira da análise de site pode ser importada em Cisco NC para ajudar no design WLAN e no desenvolvimento.

- Desenvolvimento — Um grupo largo de moldes integrados do controlador e da configuração do ponto de acesso entrega disposições rápidas e eficazes na redução de custos. O exame da rede é apoiado para o gerenciamento de configuração eficaz. Os NC igualmente fornecem ferramentas para ajudar na monitoração, promovendo, e Access point (autônomos) autônomos do Cisco Aironet da migração para operar-se como o Lightweight Access Points e a corrida CAPWAP. o controle de acesso Papel-baseado fornece a flexibilidade segmentar a rede Wireless em uns ou vários domínios virtuais controlados por uma única plataforma de Cisco NC.
- Monitoração e Troubleshooting — A monitoração centralizada das ajudas inteiras WLAN mantém o desempenho robusto WLAN e uma experiência wireless ótima. Cisco CleanAir fornece a informação detalhada sobre eventos da interferência RF, qualidade do ar, e ameaças de segurança da interferência para ajudar mais eficientemente a avaliar, dar a prioridade, e controlar a edições da interferência RF. Os indicadores gráficos fáceis de usar servem como um ponto de início para a manutenção, a Segurança, o Troubleshooting, e o planejamento da capacidade futuro. Os gráficos, as cartas, e as tabelas são interativos para a configuração rápida e a reconfiguração. As árvores hierárquicas, o código de cores, e os ícones do mapeamento apoiam avaliações rápidas do visualização e do estado da rede, dos dispositivos, e da qualidade do ar. o sumário Nunca-atual do alarme fornece a falha, o evento, e o Gerenciamento robustos do alarme. A ferramenta de pesquisa persistente facilita o acesso da cruz-rede à informação imediata e histórica sobre os dispositivos e os ativos situados em qualquer lugar na rede de acesso, incluindo atributos do valor-limite e de sessão, história da associação, local de ponto final, desempenho RF, estatísticas, Radio Resource Management (RRM), e qualidade do ar. Uma ferramenta de Troubleshooting incorporado do cliente fornece um método passo a passo para analisar problemas para todo o prendido e dispositivos do cliente Wireless. As ajudas robustas desta ferramenta de Troubleshooting do cliente reduzem custos operacionais apressando a definição das documentações de problema para uma variedade de tipos de dispositivo do cliente do Wi-fi.

O papel dos NC na rede

Esta figura descreve a arquitetura de rede do Cisco Wireless com prima NC de Cisco. As interações entre os vários elementos de rede, que são controlador do Wireless LAN, AP, interruptor do Cisco catalyst, Serviços de mobilidade motor, Sistema de controle de redes, estação de gerenciamento da rede cliente, e aplicativo de terceiros.



Portas usadas por NC

Source Device	Destination Device	Protocol	Destination Port	Description
NCS	WLC and MSE	TCP	21	FTP - Used to transfer files to/from devices
Various Management Stations	NCS Host Server OS-Linux	TCP	22	SSH - Used for remote Host Access
NCS	a IOS AP	TCP	23	Telnet - Used for a IOS AP Configuration
NCS	SMTP mail servers	TCP	25	SMTP – used for fault notifications
AAA Servers	NCS	TCP/UDP	49	TACACS+
NCS	a IOS AP	UDP	53	DNS – used for a IOS AP Configuration
WLC	NCS	UDP	69	TFTP - Used to transfer files to/from devices
Various Management Stations	NCS	TCP	80	HTTP (Configurable at install time)
NTP Server	WLC	UDP	123	NTP
WLC and MSE	NCS	UDP	161	SNMP discovery, inventory a IOS AP and others
WLC and MSE	NCS	UDP	162	SNMP Trap Receiver
Various Management Stations	NCS	TCP	443	HTTPS (Configurable at install time)
MSE	NCS	TCP	443	SOAP/XML (Simple Object Access Protocol Used for MSE Management
WLC	NCS	UDP	514	Syslog (Optional)
NCS HA Server	NCS	TCP	1522	HA DB Port
AAA Servers	NCS	UDP	1812 / 1645	RADIUS
AAA Servers	NCS	UDP	1813 / 1646	RADIUS
MSE	NCS	TCP	8001	MSE Data Sync. Communication Port
HA Web Server	NCS	TCP	8082	HA Web Server Port: Health Monitor for NCS HA
Various Management Stations	NCS	TCP	8456	HTTP Connector
Various Management Stations	NCS	TCP	8457	HTTP Redirect
Various Management Stations	NCS	TCP	16113	NMSP TLS Port

Suporte do dispositivo e versões de software

tipo de dispositivo	Software suportado Version*
Cisco Catalyst 2000 Series Switch: 2960, 2975	Independente do software release do ® do Cisco IOS
Cisco Catalyst 3000 Series Switch: 3560, 3750-E, 3750-X	Independente do Cisco IOS Software Release
Cisco Catalyst 4500 Series Switch	Independente do Cisco IOS Software

	Release
Cisco Catalyst 6000 Series Switch	Independente do Cisco IOS Software Release
Cisco 2x00, 4x00, wireless WLAN integrado 5500 controladores (WLCM, WiSM, WiSM2)	4.2.x, 6.x, 7.x
Cisco Aironet AP autônomos	Cisco IOS Software Release 12.3(7)JA e Mais Recente

* - os software release apoiados do controlador são alistados em Release Note NC.

Os NC têm duas opções de distribuição:

1. ferramenta de hardware
2. dispositivo virtual

O dispositivo virtual é um arquivo dos ÓVULOS que possa ser distribuído em VMware ESX/ESXi 4.x e 5.0. Esta tabela fornece números da escala para os dispositivos controlados por NC.

Escala de plataforma				
	AP unificados	aIOS AP	Switches	Controladores do Wireless LAN
Dispositivo virtual pequeno	3,000	1,000	1,000	240
Dispositivo virtual médio	7,500	2,500	2,500	600
Grande dispositivo virtual	15,000	5,000	5,000	1,200

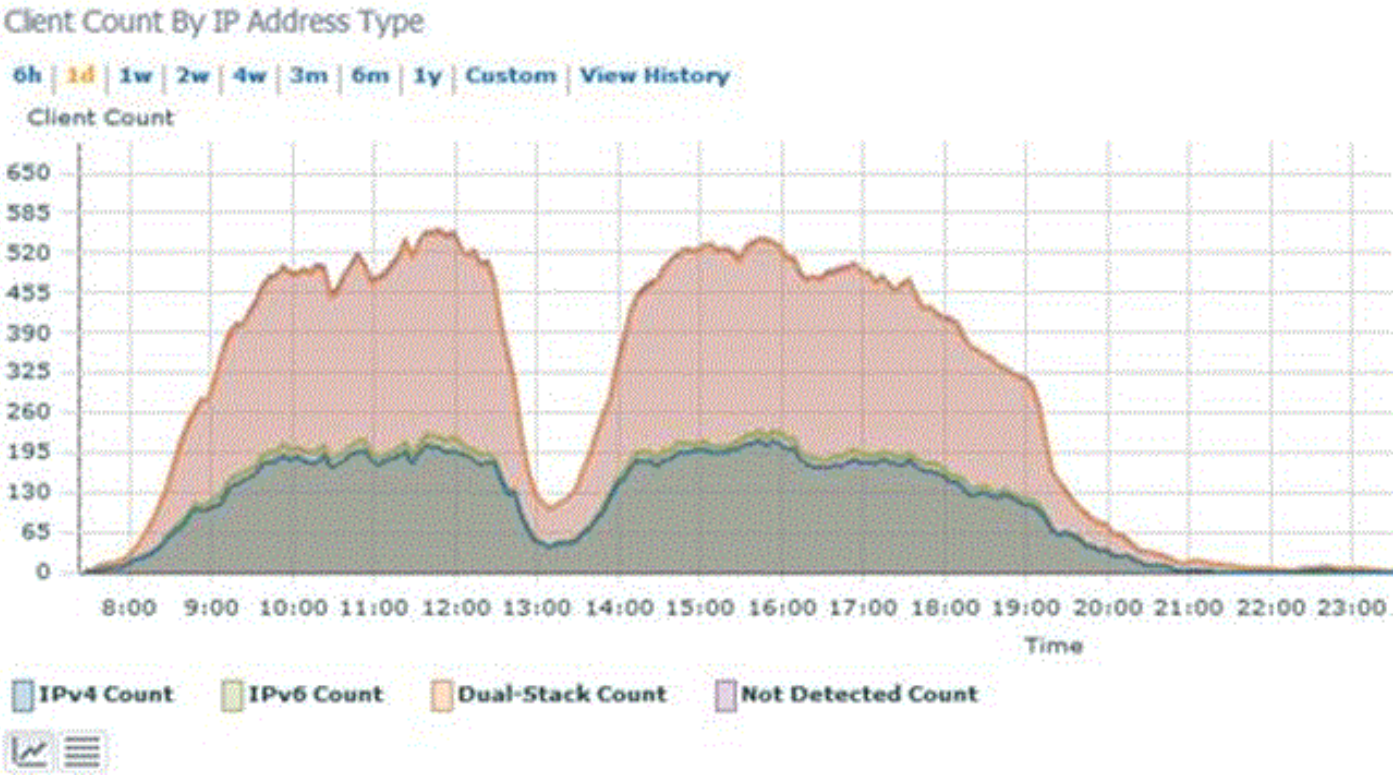
Nota: Números da escala de plataforma para os controladores do Wireless LAN (WLC; s) é escala máxima. Os WLC não contam contra NC licenciam a contagem.

Esta tabela alista os requisitos de hardware para o dispositivo virtual baseado escala prendida/wireless.

Dispositivo virtual – Requisitos de hardware			
	Processador	DRAM	Disco rígido
Dispositivo virtual pequeno	2 núcleos @ 2.93GHz	8 GB	200 GB
Dispositivo virtual médio	4 núcleos @ 2.93GHz	12 GB	300 GB
Grande dispositivo virtual	8 núcleos @ 2.93GHz	16 GB	400 GB

Home Page NC

Os NC 1.1 fornecem a capacidade para monitorar clientes do IPv6. Um dashlet novo do Home Page, contagem do cliente pelo tipo do endereço IP de Um ou Mais Servidores Cisco ICM NT, fornece um indicador visual dos clientes baseados no tipo do endereço IP de Um ou Mais Servidores Cisco ICM NT. `Não detectado` refere os clientes cujo o endereço IP de Um ou Mais Servidores Cisco ICM NT não pode ser determinado; clientes tipicamente prendidos nos casos onde a espião do IPv6 não é disponível/apoiada no dispositivo.



Suporte de navegador

Os NC 1.1 apoiam estes navegadores:

- 3.6 e mais recente de Firefox
- Google Chrome 12.0.742.x
- Microsoft Internet explorer com encaixe de Chrome**Nota:** O internet explorer nativo não é apoiado.

Este documento fornece a compreensão e o guia de projeto arquitetónicos para disposições NC.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

A informação neste documento é baseada na prima NC 1.1 de Cisco.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

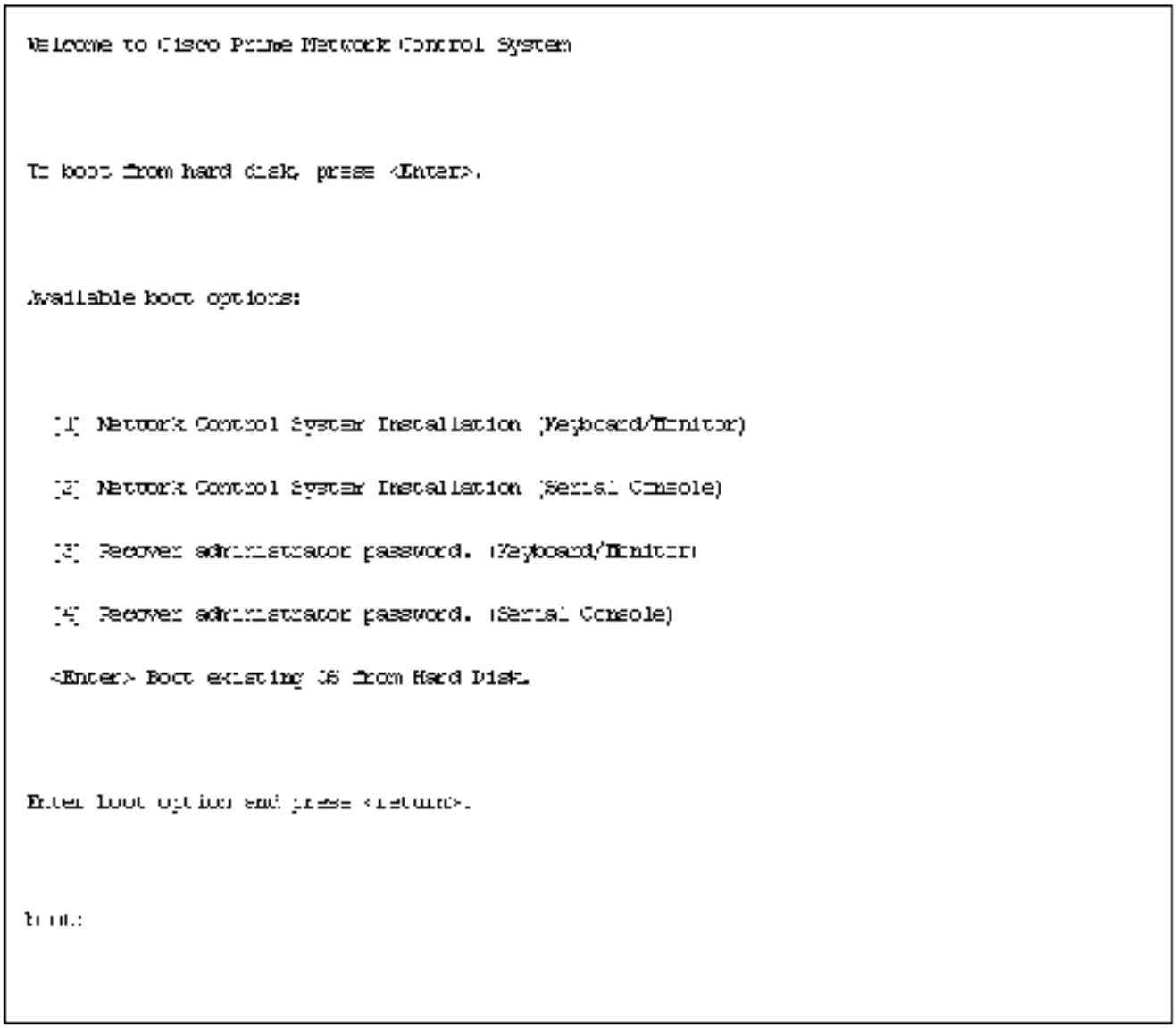
Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Instalação

Dispositivo físico: A instalação ISO

Os NC estão disponíveis como o dispositivo físico e virtual. Esta seção fornece as etapas para instalar a imagem ISO em um dispositivo físico.

1. Transferência e queimadura ISO ao DVD. O ISO é afixado no software da transferência (clientes registrados somente). Use seu nome de usuário e senha do cisco.com.
2. Instale o ISO. Recarregue a máquina com o ISO introduzido. Este indicador aparece. Escolha a opção 1 ou 2, que depende de como você é conectado ao dispositivo



3. A instalação toma aproximadamente 30 minutos para terminar. Depois que a imagem ISO é instalada, as repartições do server. Depois que seu dispositivo recarrega, vá à seção de instalação física do dispositivo do /virtual.

Dispositivo virtual: A instalação dos ÓVULOS de VMware

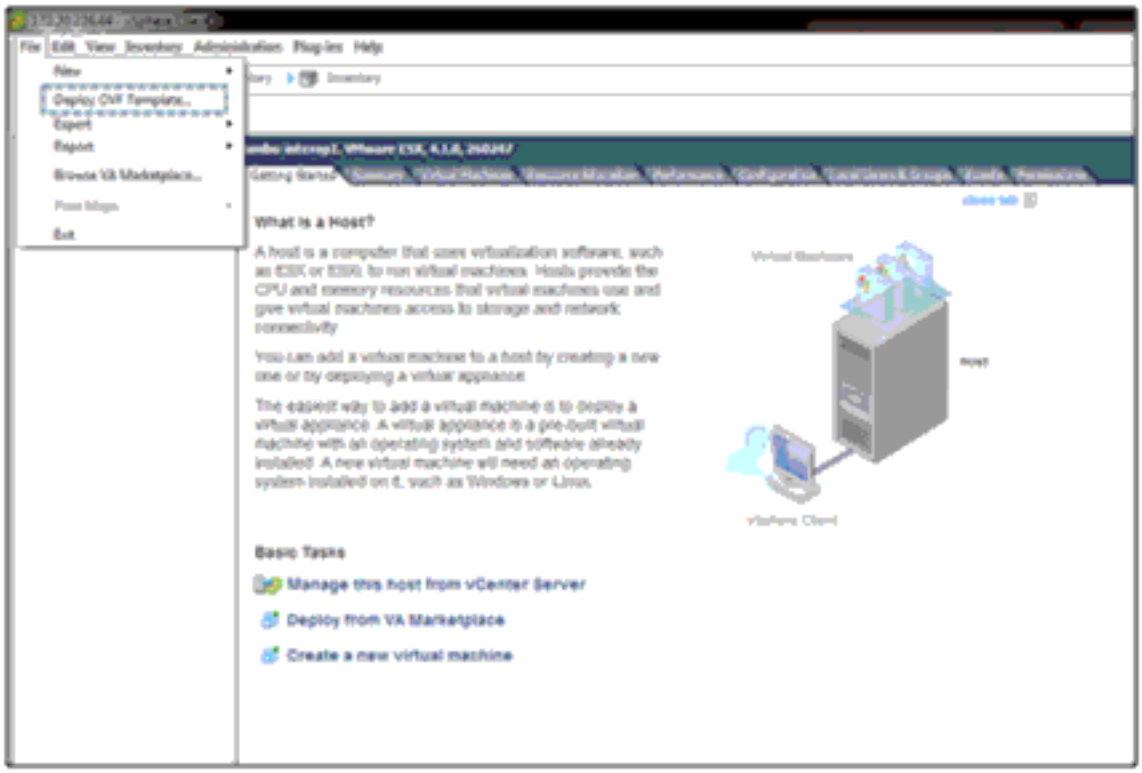
Termine estas etapas nesta seção a fim distribuir ÓVULOS em VMware ESX/ESXi 4.x. Depois que os ÓVULOS foram instalados, continue com a seção de instalação física do dispositivo do /virtual. O tempo onde toma para distribuir varia baseado na velocidade de conexão de rede ao host ESX.

Distribua o arquivo dos ÓVULOS. Os ÓVULOS são afixados no software da transferência (clientes registrados somente). Transfira os ÓVULOS apropriados baseados no número de dispositivos que é controlado por este server NC.

Use o cliente do vSphere para instalar ÓVULOS

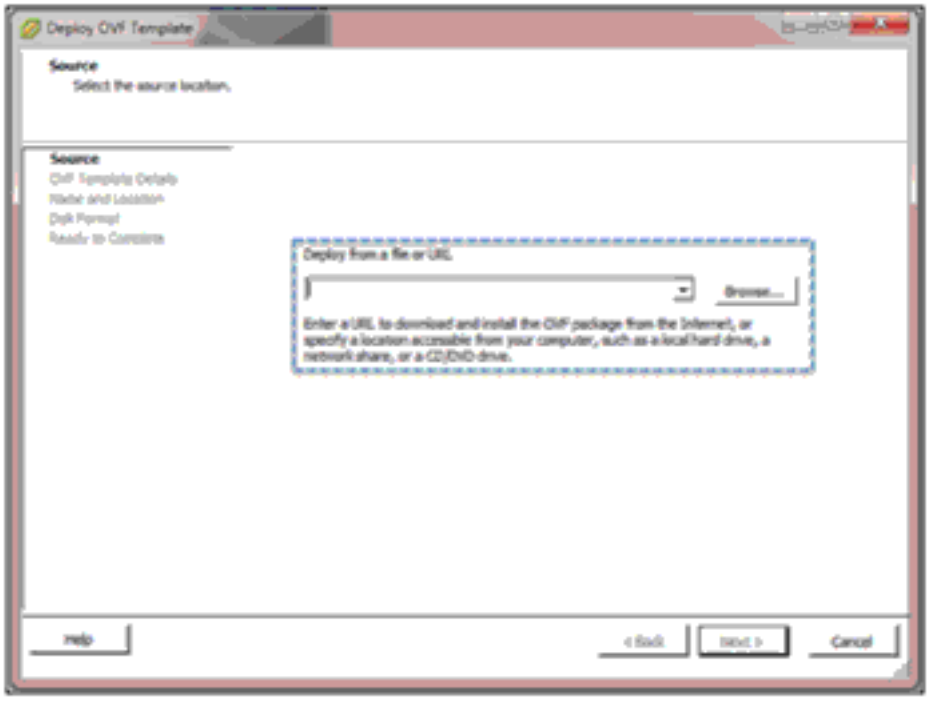
Conclua estes passos:

1. Lance o cliente do vSphere de VMware. Escolha o **arquivo > distribuem o molde**



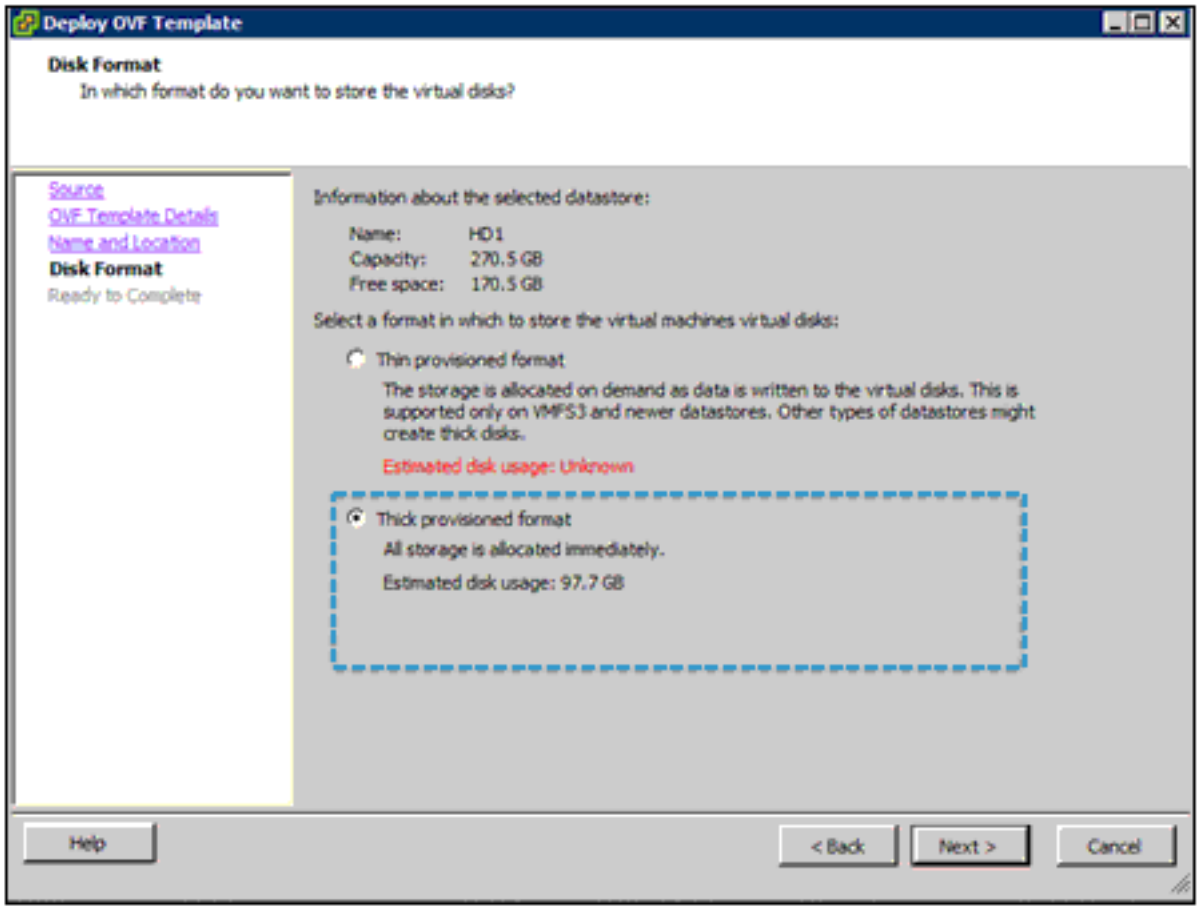
OVF. A imagem NC VMware está empacotada enquanto os ÓVULOS (arquivo aberto da virtualização) arquivam. O item de menu no tiro de tela precedente é para um molde OVF. Os ÓVULOS são uma coleção dos artigos em um único arquivo. Estes artigos consistem tipicamente em um arquivo da descrição da máquina virtual (*.ova), em um arquivo manifesto (*.mf), e no arquivo virtual do disco rígido (*.vmdk).

2. Escolha **consultam** e encontram o arquivo dos ÓVULOS NC. Clique em



Next.

3. Depois que o arquivo dos ÓVULOS é selecionado, VMware ESX/ESXi lê os atributos de arquivos dos ÓVULOS. Continue com as etapas escolheu os ÓVULOS arquivam que você quer instalar em ESX/ESXi. Na página do formato do disco, escolha a opção **fornecida grossa do formato**.



4. A página de sumário alista as opções que foram escolhidas. Clique em Next. Repartições NC. Depois que a máquina virtual foi construída, aparece no lado esquerdo do indicador. A fim lançar a máquina virtual, escolha-a do menu da mão esquerda que alista as máquinas virtuais instaladas e clique-o o ícone **aberto do console**. Neste momento, os NC são instalados como a máquina virtual. O resto das etapas da instalação é idêntico para uma máquina física e virtual.

Elevação física do dispositivo do /virtual

Conclua estes passos:

1. Obtenha a URL do local de arquivo onde a imagem de upgrade NC é armazenada no server. Execute estes comandos a fim promover a instalação NC:`ncs1/admin# ncs stop`
```
Stopping Network Control System...
This may take a few minutes...
Network Control System successfully shutdown.
```
2. Uma vez que os NC foram parados, incorpore o modo de configuração e coloque o local de arquivo URL no repositório:`ncs1/admin# conf t`
```
Enter configuration commands, one per line.  End with CNTL/Z.
ncs1/admin(config)# repository NCS58
ncs1/admin(config-Repository)# url http://xxxx/sanity/1.X.X.10/wcs-cars-appbundle/
ncs1/admin(config-Repository)# exit
ncs1/admin(config)# exit
```
3. Verifique que o repositório alcança o arquivo especificado com a URL mais cedo:`ncs1/admin# show repository NCS58`
```
ncs-upgrade-bundle-1.1.0.58.tar.gz
```
4. Execute estes comandos a fim iniciar o processo de upgrade do repositório.`ncs1/admin# application upgrade ncs-upgrade-bundle-1.1.0.58.tar.gz NCS58`
```
Save the current ADE-OS running configuration? (yes/no) [yes] ? yes
Generating configuration...
```

```
Saved the ADE-OS running configuration to startup successfully
Initiating Application Upgrade...
```

5. Uma mensagem deve aparecer que indique que o processo de upgrade está agora completo.

Começando NC

Depois que o server recarrega, registre no sistema como o admin usando a senha que você forneceu como parte da etapa da instalação. Depois que você registrou no server, ligue o server NC com `admin@ncs-server optar] # comando start dos ncs.`

Os mensagens do console indicam quando os NC estão sendo executado. Registre em seus NC o server através do navegador da Web como raiz de usuário com a senha que você escolheu durante a instalação. A senha root pode ser mudada depois que você registra em NC com o início de uma sessão do navegador.

Migração do WCS aos NC

Você deve promover seu server de Cisco WCS a uma destas liberações antes que você tente executar o processo de migração a NC 1.1.x.x.

- 7.0.164.3
- 7.0.172.0
- 7.0.220.0

Esta seção fornece instruções para que como migre o WCS em Windows ou no servidor Linux aos NC. A liberação NC é uma versão principal a prever o Gerenciamento convirgido do prendido e dispositivos Wireless, e escalabilidade aumentada. A plataforma NC é baseada no OS do bit de Linux 64, e o base de dados backend é o Oracle DBMS. As Plataformas existentes WCS são ou Windows ou Linux 32 mordido e o base de dados backend são DB contínuo.

Migração de dados do WCS

Dados da exportação do WCS

Exporte dados de WCS 7.x com o CLI. O comando CLI do **userdata da exportação** está disponível na liberação 7.x WCS e mais tarde, que cria o arquivo do .zip que contém o arquivo de dados WCS. O CLI não fornece nenhuma opção para personalizar o que pode ser exportado; todos os artigos definidos pelo utilizador NON-globais são exportados. Termine estas etapas a fim exportar dados WCS:

1. Pare o server WCS.
2. Execute o comando da **exportação** através do arquivo de script e forneça o trajeto e exporte o nome de arquivo quando alertado.
3. Para Linux, execute export.sh todo o comando de /data/wcs.zip. Para Windows, execute todos o export.bat \ comando dos dados \ wcs.zip.

Dados da migração WCS aos NC

Termine estas etapas a fim migrar dados WCS:

1. Coloque o arquivo do .zip da exportação WCS (por exemplo, wcs.zip) em um repositório ou em um dobrador (por exemplo, repositórios).
2. Entre como o usuário admin e pare o server NC inscrevendo o **comando stop dos ncs**. Configurar o repositório FTP no dispositivo NC com o **comando repository**:`ncs-appliance/admin#`**`configure`** `ncs-appliance/admin(config)#` **`repository ncs-ftp-repo`** `ncs-appliance/admin(config-Repository)#` **`url ftp://209.165.200.227//`** `ncs-appliance/admin(config-Repository)#` **`user ftp-user password plain ftp-user`** **Nota:** Certifique-se que o arquivo arquivado está disponível com o comando do **repositoryname do repositório da mostra**.
3. Incorpore os **ncs migram o** comando a fim restaurar o base de dados WCS.`ncs-appliance/admin#` **`ncs migrate wcs-data wcs.zip repository ncs-ftp-repo`**
4. Àrevelia, nenhum evento WCS é migrado. Inscreva o **comando start dos ncs** a fim ligar o server NC depois que a elevação é terminada. Entre à interface do utilizador NC com o login de raiz e a senha root.Estes dados não são migrados do WCS aos NC:Subconjunto dos relatórios — Imagem Predownload AP, de perfil AP estado, sumário AP, contagem do cliente, sumário do cliente, tráfego do cliente, relatório PCI, de conformidade PCI relatórios sumário detalhados e relatórios sumário, preferidos do atendimento da rede, AP desonestos, rogues ad hoc, rogues ad hoc novos e relatórios sumário da Segurança.Personalização do painelA informação estatísticas da estação do cliente não é povoada com dados velhos WCS em cartas dos clientes, em página dos detalhes do cliente, em painéis e em relatórios.A informação de sessão histórica do cliente obtém promovida.A história dos eventos armazenada no base de dados WCS não é migrada aos NC.O IP de servidor e as credenciais RADIUS/TACACS não estão migrados e precisam de ser adicionados outra vez depois que a migração está completa. Você precisa de copiar os atributos feitos sob encomenda os mais atrasados dos NC e de inclui-los no servidor AAA para a autenticação de usuário/autorização no TACACS+/RADIUS.**Nota:** Certifique-se que server RADIUS/TACACS está permitido como o modo AAA na página da administração > das configurações de modo AAA > AAA.Somente os alarmes com Domínio Virtual da raiz são migrados da liberação 7.0 aos NC.A senha root não é migrada da liberação 7.0.164.3 ou 7.0.172.0 à liberação 1.1.x.x NC. O usuário deve mudar a senha root durante a instalação do aplicativo. Não os usuários de raiz e suas credenciais são migrados durante a migração.As categorias e as subcategorias do alarme não são restauradas após a migração ao sumário do alarme NC.

Elevação NC de NC 1.0.x a 1.1

Você pode promover das liberações 1.0.0.96, 1.0.1.4, 1.0.2.28, e 1.0.2.29 NC a NC 1.1.x.x.

Estes artigos devem ser notados antes do processo de upgrade:

- Assegure-se de que você execute um backup antes que você tente promover.
- Alta disponibilidade do desabilitação antes que você executar a elevação.
- Feche NC antes que você execute a elevação. Execute o **comando stop dos ncs** a fim parar NC.

Use este comando a fim promover de NC 1.0 a NC 1.1.x.x:

```
# application upgrade NCS-upgrade-bundle-1.0.2.x.tar.gz wcs-ftp-repo
```

No comando precedente, **NCS-upgrade-bundle-1.1.x.x.tar.gz** é o arquivo do pacote da elevação, que está disponível no software da transferência (clientes registrados somente). O repositório usado no exemplo, WCS-FTP-**repo**, pode ser todo o repositório válido. Estes são exemplos das

configurações de repositório:

Repositório FTP:

```
#
configure (config)#
repository wcs-ftp-repo (config-Repository)#
url ftp://ip-address (config-Repository)#
user ftp-user password plain ftp-user (config-Repository)#
exit (config)#
exit #
```

Repositório SFTP:

```
# configure
(config)# repository wcs-sftp-repo
(config-Repository)# url sftp://ip-address
(config-Repository)# user ftp-user password plain ftp-user
(config-Repository)# exit (config)# exit #
```

Repositório TFTP:

```
# configure
(config)# repository wcs-tftp-repo
(config-Repository)# url tftp://ip-address
(config-Repository)# exit (config)# exit #
```

Mapas da importação do WCS

A exportação/recursos de importação do mapa está disponíveis em WCS 7.0. Esta característica é descrita em detalhe no manual de configuração WCS 7.0.

Depois que você exporta mapas de seu server WCS, você pode importar este grupo de mapas em seu server NC. As etapas para importar seus mapas são cobertas no manual de configuração WCS 7.0.

Nota: É importante que os AP em seu server WCS estão adicionados primeiramente a seu server NC antes de importar mapas desde que os AP em seus mapas WCS são incluídos igualmente durante o processo da exportação. Os AP que não foram adicionados a seus NC mas estam presente no resultado exportado dos mapas do assoalho nos erros que são indicados quando você importa aqueles mapas em NC.

Alta disponibilidade - Teoria básica da operação

A aplicação NC HA nos NC permite até dois sistemas preliminares NC falhar sobre a uns (backup) NC secundários. Um segundo server é exigido que tenha os recursos suficientes (CPU, disco rígido, conexão de rede) a fim tomar sobre a operação NC caso os NC preliminares falharem. Cada instância de base de dados nos NC secundários é um standby recente para os NC preliminares correspondentes.

A notação que é usada para descrever preliminar e os sistemas secundários são `N: M`, onde N = número de sistemas preliminares na operação e M = número de sistemas secundários que estão suportando os sistemas preliminares.

Nos NC, estas configurações HA são apoiadas:

1:1 – 1 Primary, 1 Secondary

O tamanho do servidor secundário deve ser maior do que ou igual ao servidor primário, por exemplo se o server preliminar NC é ÓVULOS médios, a seguir o server secundário NC deve ser ÓVULOS médios ou grandes.

O preliminar e o servidor secundário podem ser uma mistura de um dispositivo físico e virtual. Por exemplo, se o server preliminar NC é um dispositivo físico, o servidor secundário pode ser ou dispositivo físico ou o dispositivo virtual dos grandes ÓVULOS, por exemplo, a configuração do servidor e a cola de grandes ÓVULOS é o mesmo que o dispositivo físico.

O monitor de funcionamento (HM) é um processo novo executado nos NC, isso é o componente principal que controla a operação HA do sistema. O HM é dividido nestes submódulos múltiplos, cada qual seguram um grupo específico de funções:

- HM do núcleo — responsável para estas tarefas:configuração do sistema total HAmantém a máquina de estado para o sistema HAcomeço/parada do HM e dos NC JVMcomece/parada e monitor de outros submódulos dentro do HMsegura o registro pares preliminares/secundáriosautentica a sessão do específico do HMfaz todas as decisões sobre o failover e failback
- Batimento cardíaco — O submódulo do batimento cardíaco é responsável para manter uma comunicação entre o HMs preliminar e secundário. Uma comunicação ocorre sobre o HTTPS (a porta padrão é 8082). O valor de timeout é 2 segundos. Um mecanismo de nova tentativa foi executado para experimentar de novo o estabelecimento da Conectividade entre o P-HM e o S-HM. Se o HM não recebe uma resposta após ter enviado um pedido da pulsação do coração dentro do período de timeout, experimenta de novo o estabelecimento de uma comunicação enviando um outro pedido da pulsação do coração. O número total de novas tentativas é 3. Depois que uma comunicação tem não ser estabelecida depois que 3 novas tentativas, a ação apropriada da tomada HMs conforme as encenações definidas:o servidor primário vai para baixo: este é o exemplo clássico do Failover. Nesta encenação, quando o S-HM não recebe pedidos da pulsação do coração pelos segundos 6 (3 novas tentativas x 2 segundos), inicia o mecanismo do Failover nos NC secundários.o servidor secundário vai para baixo: nesta encenação, o P-HM não recebe a resposta da pulsação do coração do S-HM pelos segundos 6 (3 novas tentativas x 2 segundos). Quando isto acontece, o P-HM muda seu estado a PRIMARY_ALONE, levanta alarmes e muda-os no modo de escuta – esperando para receber todas as mensagens do secundário para restabelecer o link entre P-HM e HM do - S.
- Monitor do aplicativo — O submódulo do monitor do aplicativo é responsável para uma comunicação com a estrutura NC (NC JVM) no servidor local recuperar a informação de status. Uma comunicação é através do SABÃO sobre o HTTPS.
- Monitor DB — O submódulo do monitor DB configura o DB para a replicação. Não é responsável para a replicação própria DB porque este é realizado através do protocolo proprietário da replicação do base de dados.
- Sincronização do arquivo — O submódulo da sincronização do arquivo tem 4 secundário-componentes:Arquivo Archiver: faz a varredura periodicamente dos diretórios que procuram os arquivos que foram alterados. Recolhe uns arquivos e adicionar-los a um arquivo extenso TARAgente de transferência de arquivo (FTA): responsável para transferir o arquivo extenso TAR da compressa ao destino (o outro server, isto é preliminar a secundário ou a secundário a preliminar).Servlet do upload de arquivo (FUS): as corridas no servidor secundário e são as contrapartes ao FTA. Quando recebe um arquivo, o FUS flui-o diretamente ao extrator do

ALCATRÃO um pouco do que cria o arquivo no disco local (evita a atividade de disco desnecessária). O FTA e os FUS comunicam-se sobre o HTTPS.Coletor de estatísticas: mantém estatísticas de operações de transferência de arquivo do tempo que o server começa.

O base de dados NC é o elemento de armazenamento de dados do núcleo do sistema e deve ser replicated entre preliminar e sistemas de backup no tempo real do - sem perda de dados. Isto é fundamental à operação de NC HA. Os dados são armazenados em 1 de 2 maneiras:

1. Base de dados NC
2. Dados do aplicativo

Os dados do aplicativo são um grupo de arquivos planos que contenha estes dados:

- arquivo da senha do base de dados: replicated no tempo real (11 segundos)
- Arquivos de licença NC: replicated através do processamento de lote (cada 500 segundos)
- todos os arquivos sob o diretório raiz de tftp: replicated através do processamento de lote (cada 500 segundos)
- relatórios gerados programados: replicated no tempo real (11 segundos)

Monitor de funcionamento: o monitor de funcionamento (HM) é o componente principal que controla/monitora a Disponibilidade HA do sistema. Há os submódulos múltiplos que seguram várias funções com HM.

HM do núcleo: responsável para estas negociações:

- Configura o sistema HA
- Mantém a máquina de estado para o sistema do HW
- HM comece/parada
- Comece/parada e monitoram outros submódulos dentro do HM
- Segura o registro de pares preliminar-secundários
- Faz todas as decisões em relação ao failover e failback

Operação do Failover

Após a distribuição inicial dos NC, a configuração completa de NC preliminares replicated ao host dos NC secundários. Durante a operação normal (isto é os NC preliminares são operacionais), o base de dados de preliminar replicated aos NC secundários.

Além do que a replicação de base de dados, os arquivos dos dados do aplicativo igualmente replicated aos NC secundários. A frequência da replicação é 11 segundos (o tempo real do - arquiva) e 500 segundos (arquivos de lote).

Exigências NC para usar a característica NC HA

O cliente deve executar a mesma versão NC em server preliminares e secundários NC. A característica NC HA é transparente ao controlador wireless, isto é não há nenhum requisito de versão de software para o WLC, os AP e o MSE.

Configuração da característica HA

Estes parâmetros devem ser configurados nos NC preliminares:

- nome/endereço IP de Um ou Mais Servidores Cisco ICM NT de NC secundários
- endereço email do administrador de rede para a notificação do sistema
- opção do manual ou do failover automático

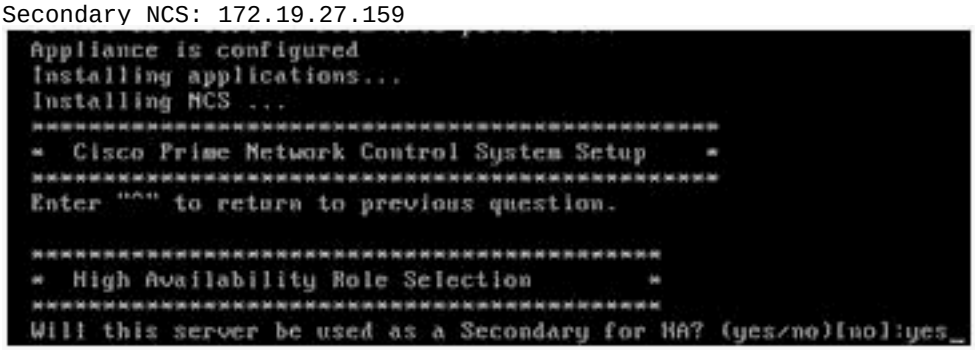
Os NC secundários devem sempre ser uma instalação nova e esta opção deve ser selecionada durante NC instala o processo. Por exemplo, os NC autônomos ou preliminares não podem ser convertidos aos NC secundários. Os NC autônomos podem ser convertidos ao HA preliminar.

Nota: A replicação de base de dados entre P-NCS e S-NCS usa a porta 1522, assim que assegure-se de que esta porta esteja aberta em todos os dispositivos de rede, tais como Firewall, Switches, Roteadores e assim por diante, ao longo do caminho de rede entre server preliminares e secundários NC.

Exemplo – A instalação e processo de configuração

Neste exemplo, este é um sistema de 1:1 NC HA

```
Primary NCS: 172.19.27.84

Secondary NCS: 172.19.27.159
```



A primeira etapa é instalar e configurar os NC secundários. Ao configurar os NC preliminares para o HA, os NC secundários precisam de ser instalados e alcançáveis pelos NC preliminares.

Nota: Um ponto chave a recordar é que quando P-NCS está sendo executado/operacional, S-NCS não está sendo executado. Quando o servidor secundário reage do modo standby, estes serviços estão sendo executado no servidor secundário: HM, Apache e base de dados. Quando P-NCS vai a um estado inativo, o HM no servidor secundário começa o processo NC JVM. Somente faz então S-NCS tornam-se acessível.

A porta do monitor de funcionamento precisa de estabelecer-se na máquina da instalação do alvo NC. O valor de porta padrão é a porta 8082. Este número de porta tem somente o significado da máquina local (porta da máquina local).

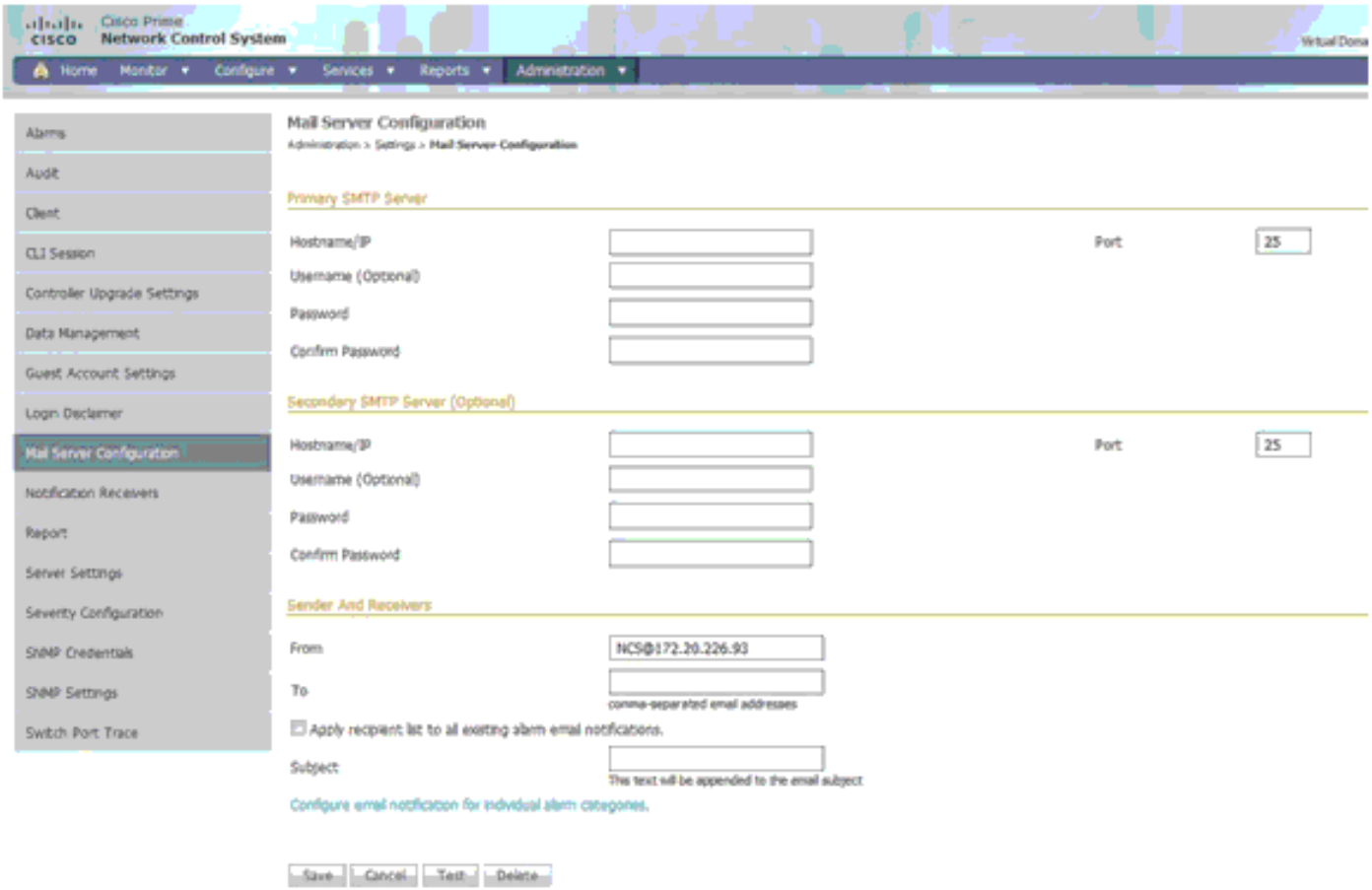
```
Check Health Monitor Port...
Please change the Health Monitor web port if needed. Health Monitor (DEFAULT: 8082):
[root@NCSlinux1NCS]#
```

A chave de autenticação para o monitor de funcionamento deve igualmente ser criada durante o processo de instalação. Esta chave é usada somente internamente pelo HM do - P e pelo HM do - S para a autenticação. Deve ser a mesma chave no preliminar e em servidores secundários.

```
Enter Authentication Key:
Enter Authentication Key again:

**************************************************
*  Summary                                       *
**************************************************
Server will be a Secondary.
Authentication Key is set.
Apply these settings? (y/n)y
Settings Applied.

Application bundle (NCS) installed successfully

 === Initial Setup for Application: NCS ===
```

Como indicado mais cedo, somente uma licença de servidor NC precisa de ser comprada. Por exemplo, uma licença separada NC não precisa de ser comprada para os NC secundários. O mesmo arquivo de licença NC reside nos NC preliminares e secundários. Desde que os NC JVM estão sendo executado somente no preliminar ou secundário (não ambos), o arquivo de licença é somente ativo em um sistema em um ponto dado a tempo.

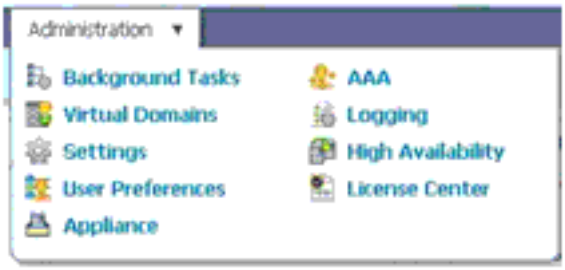
O administrador de rede igualmente precisa de fornecer ajustes do servidor de e-mail para a notificação de Email para o processo HA. Isto é exigido para a operação manual HA (intervenção do gerenciador de sistema). Navegue a esta página como segue: **>Settings > mail server da administração**

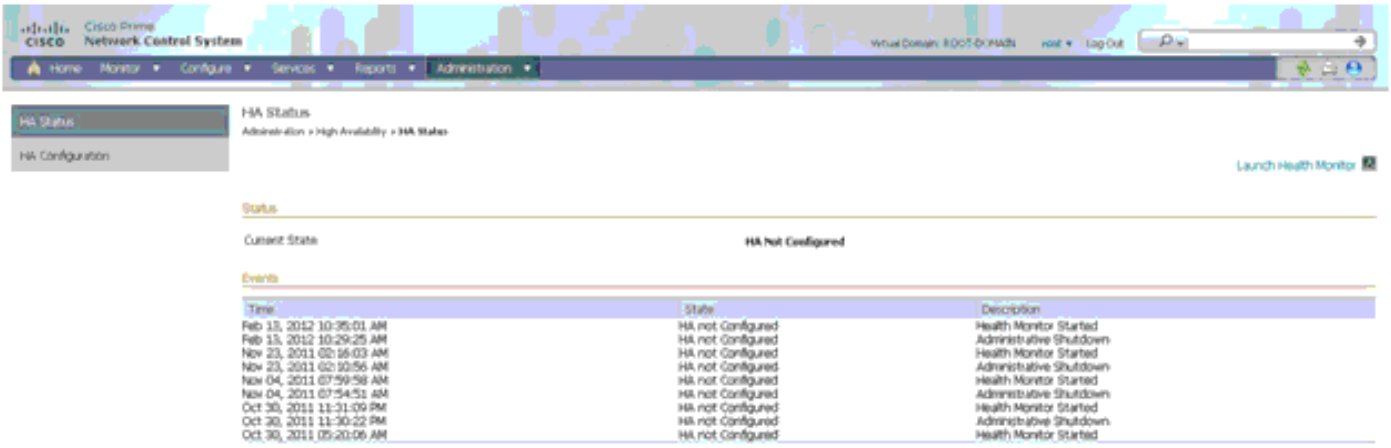


Configuração nos NC preliminares secundários

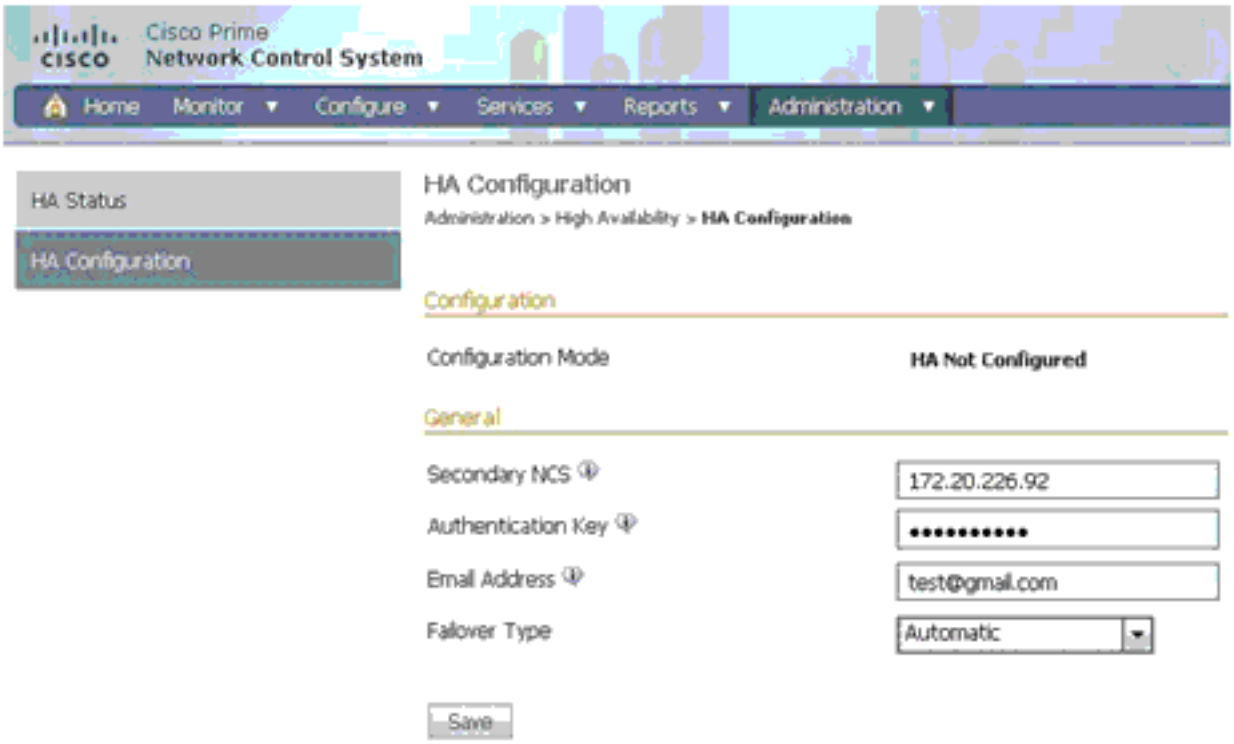
Ajustes NC

Escolha a **Disponibilidade do >High da administração**. Como destacado, o HA não é configurado atualmente neste sistema.





Do menu no lado esquerdo da tela, escolha a **configuração HA**. Isto toma-o a este indicador. Quando você incorpora a informação pedida à seção geral do título e clica a **salvaguarda & o botão Enable Button**, a configuração salvar e o HA é permitido.



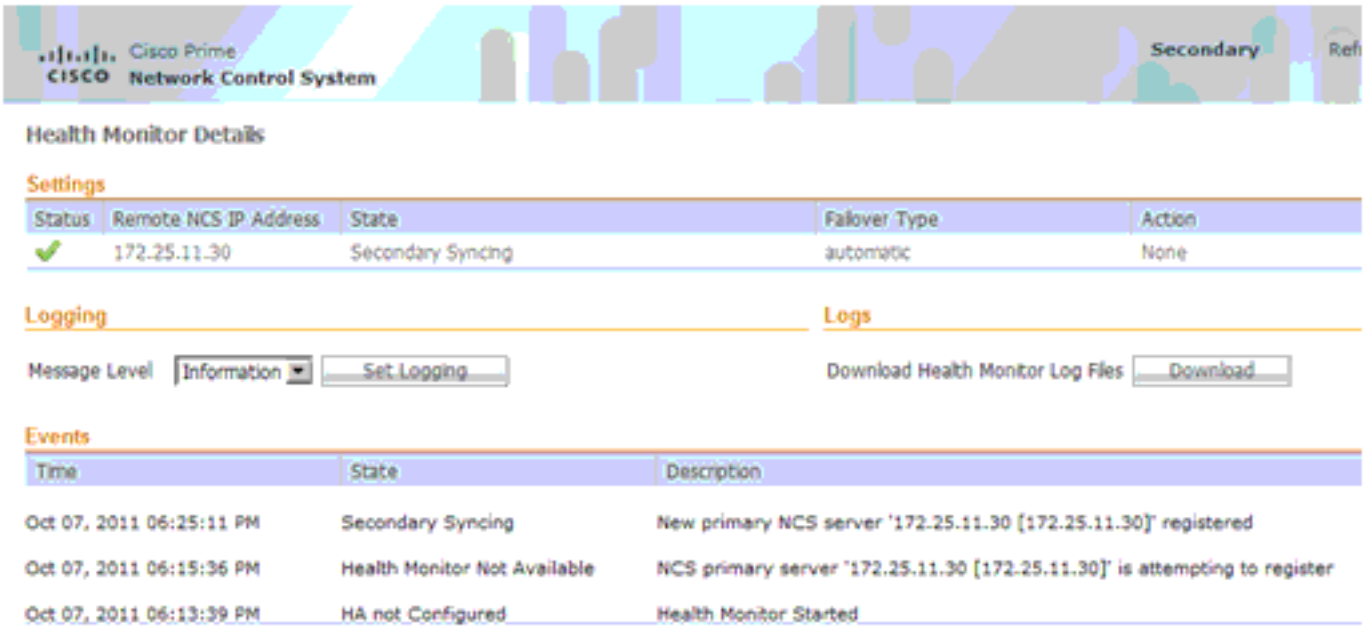
Você precisa de entrar esta informação: Endereço IP de Um ou Mais Servidores Cisco ICM NT de S-NCS, chave de autenticação, endereço email para que as notificações sejam enviadas, tipo do Failover. Você pode escolher salvar esta informação sem permitir o HA, ou salvar e permita o HA.

Monitorando a operação NC HA

Depois que você termina a etapa precedente, a informação de status de mensagem nos NC fornece a informação na configuração HA e se está permitida.

Monitor de funcionamento – NC secundários

Na tela de monitor de funcionamento nos NC secundários, você pode ver a informação de estado de NC secundários e do tipo do Failover que foi configurado. Igualmente isto permite que o administrador de rede ajuste o tipo do nível de mensagem de registro e a capacidade capturar/arquivos de registro da transferência. Você pode igualmente ver os eventos vistos por S-HM com os selos de tempo associados.



Exemplo da falha principal – Failover manual

Neste exemplo, os NC secundários foram configurados com failover manual. Por exemplo, o administrador de rede é notificado através do email que os NC preliminares tinham experimentado `para baixo uma` circunstância. O monitor de funcionamento em NC secundários detecta a condição de falha de NC preliminares. Desde que o failover manual foi configurado, o administrador de rede precisa de provocar manualmente S-NCS para tomar sobre a funcionalidade NC dos NC preliminares. Isto é feito se você registra em S-HM. Mesmo que S-NCS não esteja sendo executado, S-HM pode ser conectado a direto esta sintaxe:

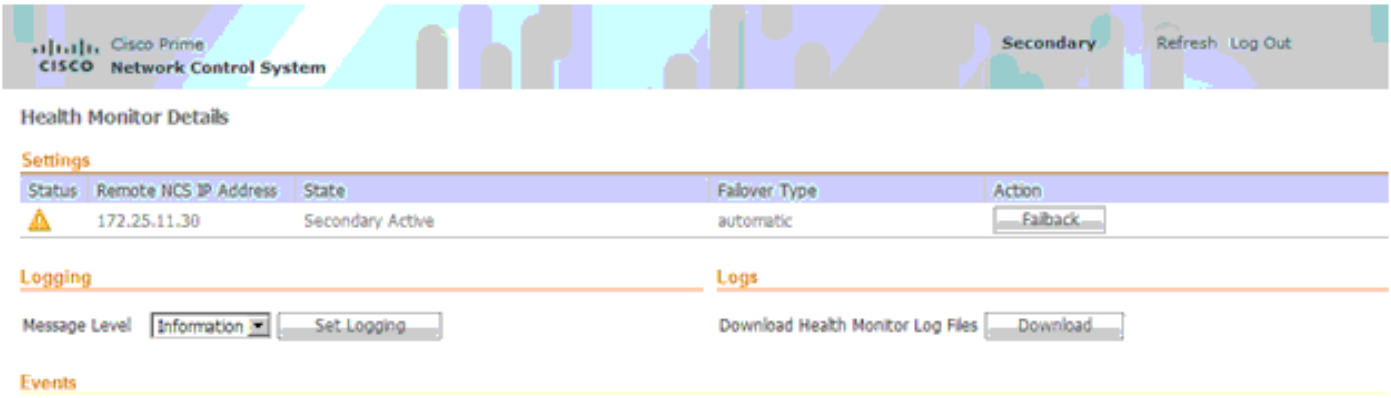
```
https://<SNCS_ip_address>:HM_port/
```

O S-HM indica mensagens com respeito aos eventos que são considerados. Desde que o failover manual foi configurado, o S-HM espera o administrador de sistema para invocar o processo do Failover. Uma vez que o failover manual foi escolhido, esta mensagem está indicada enquanto S-NCS começa. Uma vez que o processo do Failover esteve terminado, assim que significa que o processo da replicação de base de dados NC está terminado e processo S-NCS JVM começou, a seguir S-NCS é os NC ativos.

O monitor de funcionamento nos NC secundários fornece a informação de status dos NC preliminares e dos servidores secundários. O failback pode ser iniciado com S-HM uma vez que P-NCS recuperou da condição de falha. *O processo do failback é iniciado sempre manualmente* a respeito de evita uma condição do flapping que possa às vezes ocorrer quando há um problema de conectividade de rede.

Failback

Quando as edições no server que hospedam P-NCS foram resolvidas, o failback pode manualmente ser iniciado. Uma vez que isto é feito, a tela está indicada em S-NCS. Quando você inicia o failback, o base de dados NC em S-NCS e algum outros arquivos que mudaram desde que S-NCS tomou sobre a operação NC estão sincronizados entre S-NCS e P-NCS. Uma vez que a sincronização de base de dados foi terminada, P-NCS JVM está começado por P-HM. Quando P-NCS JVM está sendo executado, esta tela é indicada em S-HM.



Failover automático

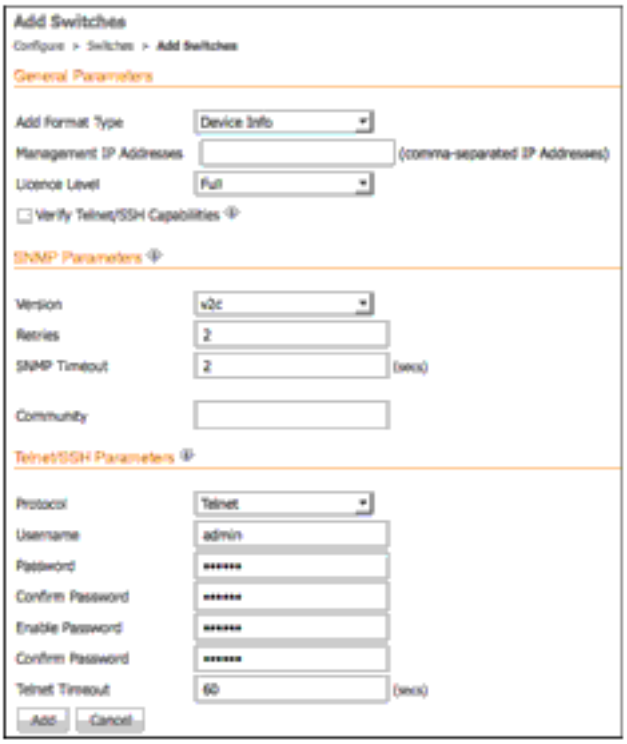
O failover automático é um processo muito mais simples. Todas as etapas de configuração são as mesmas a não ser que o *failover automático* seja selecionado. Uma vez que configurado, o administrador de rede não precisa de interagir com o HM do - S para que a operação do Failover ocorra. Somente durante o failback é a intervenção humana exigida.

Adicionar um controlador aos NC

- Escolha **configuram > controlador do > Add dos controladores** a fim adicionar um interruptor. Os controladores do Cisco Wireless (WLC) podem ser adicionados em manualmente ou através do arquivo CSV.
- Depois que você adiciona os controladores, estão colocados temporariamente na página do monitor > dos dispositivos desconhecidos quando os NC tentarem se comunicar com os controladores que você adicionou. Uma vez uma comunicação com o controlador foi bem sucedida, os movimentos do controlador da página do monitor > dos dispositivos desconhecidos à página do monitor > dos controladores. Se os NC não podem se comunicar com sucesso com um controlador, permanece no monitor > nos dispositivos desconhecidos e uma condição de erro é indicada.

Adicionar um interruptor aos NC

Escolha **configuram > Switches do > Add do Switches** a fim adicionar um interruptor. O Switches pode ser adicionado individualmente ou os switch múltiplos podem ser importados através do arquivo CSV.



Depois que um interruptor é adicionado, está colocado temporariamente na página do monitor > do Switches quando os NC tentarem se comunicar com este interruptor. Uma vez uma comunicação com o interruptor foi bem sucedida, NC move o interruptor da página do monitor > dos dispositivos desconhecidos para a página do monitor > do Switches. Se os NC não podem se comunicar com sucesso com um interruptor, permanece no monitor > nos dispositivos desconhecidos e uma condição de erro é indicada.

Configuração de Catalyst switch

Há três etapas para a configuração de segurança do cliente no Switches do Cisco catalyst: AAA, RAIO e autenticação 802.1x/MAC.

Configuração de AAA

```
aaa new-model
!
aaa authentication login login-none none
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa authorization auth-proxy default group radius
aaa accounting update periodic 2
aaa accounting dot1x default start-stop group radius
!
ip device tracking
```

Refira a vista geral AAA para mais informação.

Esta configuração é configuração do switch Cisco para a autenticação RADIUS para Cisco ISE/ACS e servidores Radius não-Cisco.

Configuração do IOS

```
radius-server attribute 6 on-for-login-auth
radius-server attribute 6 support-multiple
radius-server attribute 8 include-in-access-req
```

```
radius-server attribute 25 access-request include
radius-server dead-criteria time 10 tries 3
radius-server host 40.40.1.10 auth-port 1812 acct-port
1813 key secret
radius-server timeout 10
radius-server key secret
radius-server vsa send cisco-nas-port
radius-server vsa send accounting
radius-server vsa send authentication
```

Consulte estes documentos para obter outras informações:

- O servidor Radius requisita novamente na falha
- Atributo RADIUS 8 (Framed-IP-endereço) em pedidos do acesso
- Referência de comandos do Cisco IOS Security

802.1X e configuração do AUTH MAC — Esta configuração de switch fornece três funções: a autenticação para clientes do 802.1x, permite que os clientes continuem na rede que falham a autenticação do 802.1x (o evento é gerado/enviado aos NC para a autenticação falhada do 802.1x), o desvio da autenticação de MAC (MAB) para os dispositivos IP que não têm o suplicante do 802.1x.

Configuração do IOS da Cisco

```
dot1x system-auth-control
interface <interface>
 description *** Dot1x Client ***
 switchport mode access
 authentication port-control auto
 authentication open
 < - monitor mode: allows client on the network if it
fails 802.1x auth dot1x pae authenticator mab
authentication order mab dot1x <- for devices without
802.1x capability or credentials !
```

Refira configurar a autenticação com base na porta do IEEE 802.1X para mais informação.

Notificação MAC para armadilhas (clientes da NON-identidade) — este do Cisco IOS dos recursos de switch SNMP traps para a frente do interruptor ao NMS, por exemplo, server NC, para notificações MAC, clientes non-802.1x.

Configuração do IOS da Cisco

```
mac address-table notification change interval 5
mac address-table notification change history-size 10
mac address-table notification change

interface <interface>
 description non-identity clients
 switchport access vlan <VLAN ID>
 switchport mode access
 snmp trap mac-notification change added  <- interface
level config for MAC Notification
  snmp trap mac-notification change removed <- interface
level config for MAC Notification
```

Os comandos Debug debugam pacotes SNMP

Mudança da notificação da tabela de endereços MAC da mostra dos comandos show

Refira configurar armadilhas da notificação de alteração MAC para mais informação.

A configuração do Syslog (clientes da identidade somente) — esta configuração encaminha mensagens do syslog do Catalyst Switch ao server NC.

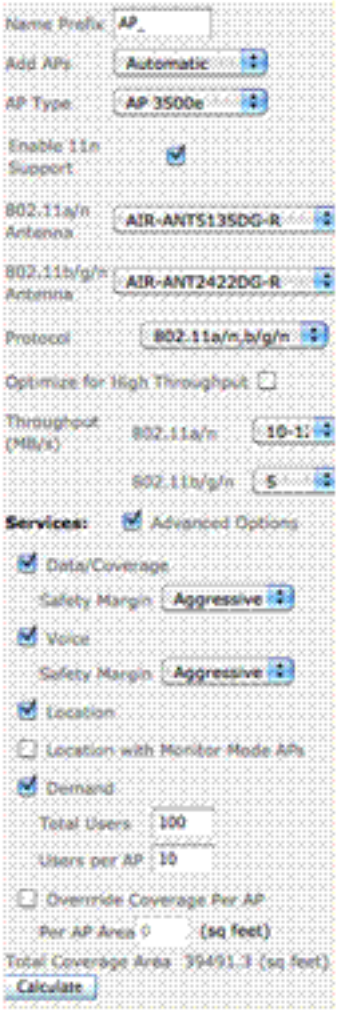
Configuração do IOS
archive log config   notify syslog contenttype plaintext logging facility auth logging <IP address of NCS server>

Planeamento de rede Wireless

Ferramenta planejando

A ferramenta incorporado do planeamento fornece uma maneira para administradores de rede em determinar o que é exigido no desenvolvimento de uma rede Wireless. Como parte do processo de planejamento, os vários critérios são entrados na ferramenta do planeamento. Conclua estes passos:

1. Especifique o método do prefixo AP e da colocação AP (automático contra o manual).
2. Escolha o tipo AP e especifique a antena para a faixa 2.4GHz e 5GHz.
3. Escolha o protocolo (faixa) e a taxa de transferência desejada mínimo pela faixa que é exigida para este plano
4. Permita o modo do planeamento para as opções avançadas para dados, Voz, lugar. Os dados e a Voz fornecem margens de segurança para a ajuda do projeto. As margens de segurança ajudam a projetar com certeza pontos iniciais RSSI, que é detalhado na ajuda online. O lugar com modo de monitor fatora no AP que poderia ser distribuído para aumentar a precisão do lugar. O lugar exige tipicamente um desenvolvimento mais denso do que os dados e a caixa de seleção do lugar ajudam o plano para a precisão anunciada do lugar.
5. As opções da *procura* e da *ultrapassagem* permitem planejando para todos os casos especiais onde há um alto densidade da presença do cliente tais salas de conferência ou



salões de leitura. A proposta gerada contém estes:Detalhes do plano horizontalNegação/espaço/suposiçõesColocação proposta APCobertura e taxa de dados HeatmapAnálise da cobertura

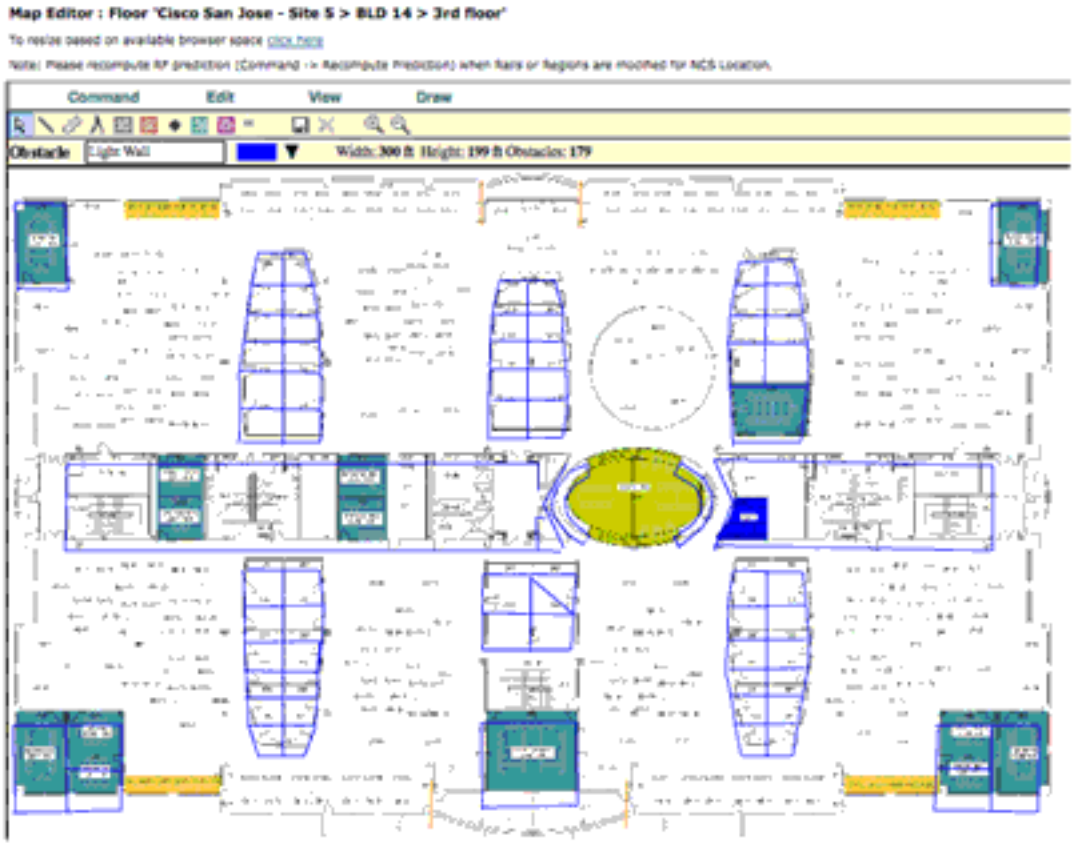
Editor do mapa

O editor integrado do mapa nos NC esclarece objetos e obstáculos em um assoalho. A alteração de características do mapa do assoalho conduz a um modelo mais preciso da propagação RF que seja indicado em mapas com caráter de previsão do calor. As características da atenuação para objetos e o motor com caráter de previsão da ajuda dos obstáculos indicam um mapa com caráter de previsão mais realístico do calor. edita feito para pavimentar ajudas do mapa especificam áreas e regiões como:

- Área de cobertura e marcadores — usados para notificações do lugar
- Perímetro — define o limite exterior
- Regiões da inclusão e da exclusão do lugar — usadas para eventos e notificações do lugar

Objetos e obstáculos que podem ser especificados:

- Paredes (luz e pesado) — 2dB e 13dB
- Compartimento (paredes) — 1dB
- Portas (luz e pesado) — 4dB e 15dB
- Vidro (portas, indicadores, paredes) — 1.5dB



Mapas da importação do WCS aos NC

A exportação/recursos de importação do mapa está disponíveis em WCS 7.0. Esta característica é descrita em detalhe no manual de configuração WCS 7.0.

Após a exportação dos mapas do server da fonte WCS, este grupo de mapas pode ser importado no server do destino NC. As etapas para importar seus mapas são cobertas no manual de configuração NC.

Nota: É importante que os AP no server WCS estão adicionados primeiramente ao server NC antes de importar mapas desde que os AP nos mapas WCS são incluídos igualmente durante o processo da exportação. Os AP que não foram adicionados a seus NC mas estam presente no resultado exportado dos mapas do assoalho nos erros que estão sendo indicados quando você importa aqueles mapas em NC.

Use NC para distribuir um Wireless LAN

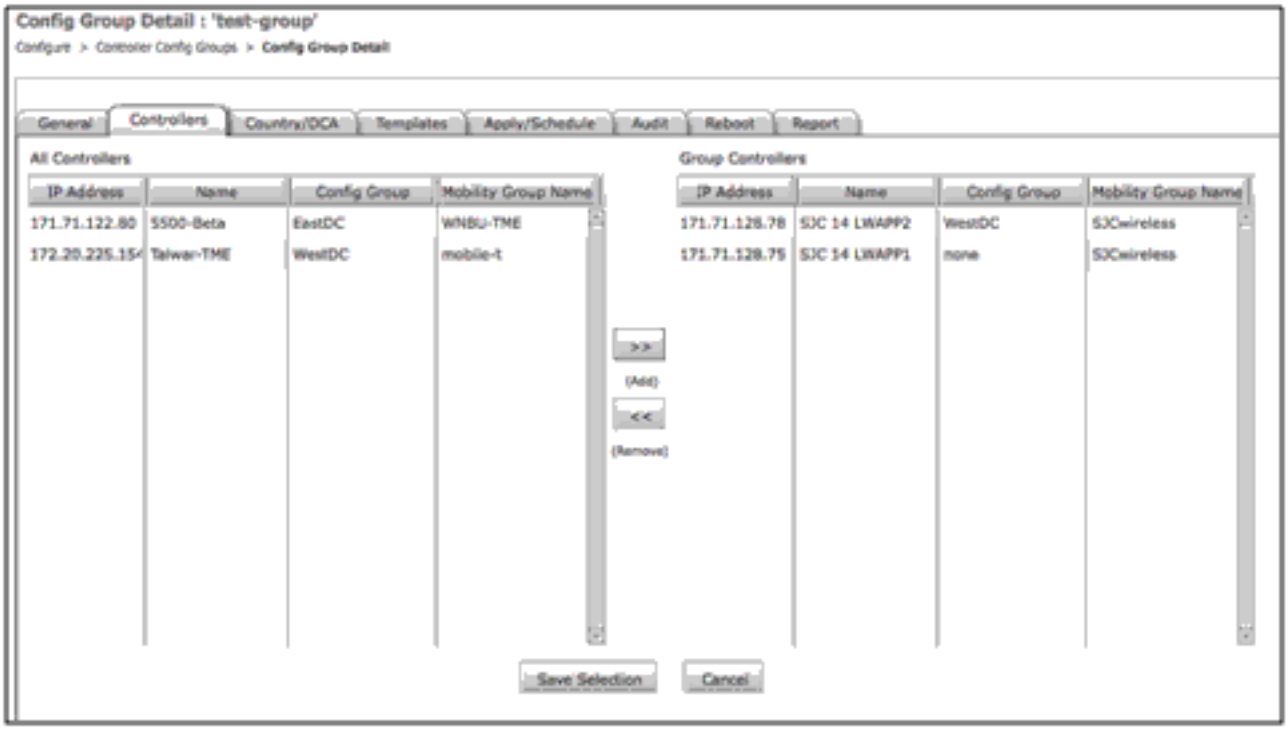
Gabaritos de configuração

Os gabaritos de configuração são grupos de configurações que podem ser aplicadas aos dispositivos a sistema ou nível global. Podem ser reutilizados a fim alterar configurações existentes. Os moldes podem igualmente ser usados para replicate a configuração aos outros dispositivos adicionados subseqüentemente. Os gabaritos de configuração podem ser usados para programar alterações de configuração na data e hora predefinida. As capacidades da auditoria nos NC podem igualmente leverage moldes da configuração para determinar diferenças da configuração entre NC e configuração de controle existente.

Grupos de configuração (Configuração-grupos)

os Configuração-grupos são uma maneira fácil agrupar logicamente controladores. Esta característica fornece uma maneira de controlar controladores com configurações similares. Os moldes podem ser extraídos de controlador existente para provision controladores novos ou controladores existentes com parâmetros de configuração adicionais. Os grupos da configuração podem igualmente ser usados para programar grupos da configuração de ser fornecida. As repartições do controlador podem igualmente ser programadas/conectado segundo requisitos operacionais. Os Grupos de mobilidade, o DCA, e o exame da configuração de controle podem igualmente ser controlados usando configuração-grupos.

Os Configuração-grupos são usados ao agrupar locais junto para um Gerenciamento mais fácil (Grupos de mobilidade, DCA e ajustes do domínio regulatório) e programando alterações de configuração remotas. Locais dos grupos para assegurar a conformidade com políticas da configuração.



- Adicionando controladores — Os controladores no WCS são apresentados e podem ser movidos sobre para recentemente o grupo da configuração
- Aplicando moldes — Descoberto ou já apresente moldes pode então ser aplicado ao controlador
- Examinar — Ensure molde-baseou a auditoria é selecionada em ajustes da auditoria e examina então controladores no grupo para assegurar-se de que seguissem com as políticas

O uso NC monitorar/pesquisa defeitos uma rede Wireless

RRM /CleanAir

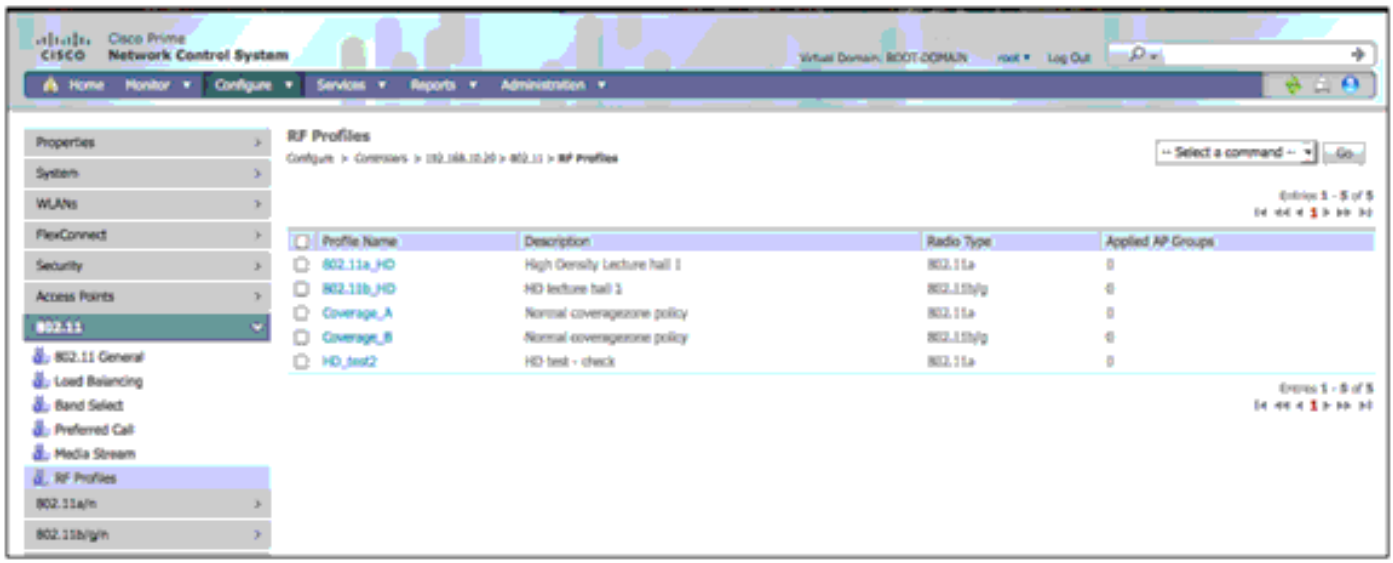
Os perfis e os grupos RF são apoiados na versão 1.1 NC para ambos os moldes da criação do perfil RF, e nos moldes do grupo AP. Se você usa NC 1.1 para criar os perfis RF através da criação dos moldes, este dá ao administrador uma maneira simples criar consistentemente e aplicar moldes aos grupos de controladores. Os fluxos de processo o mesmos que foi discutido previamente no conjunto de recursos do controlador com algumas diferenças menores mas importantes.

O processo é o mesmo que discutido previamente que você cria primeiramente perfis RF, a seguir aplica os perfis através dos grupos AP. As diferenças estão em como esta é feita dos NC e no uso dos moldes distribuir através da rede.

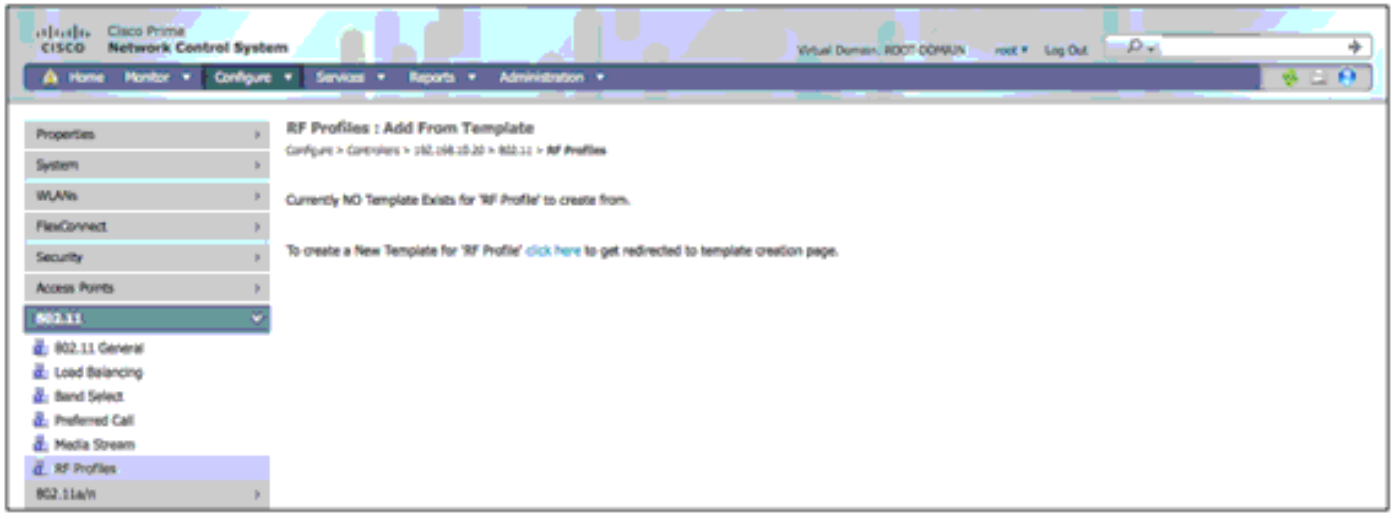
Construa um perfil RF com prima NC 1.1 de Cisco

Na prima NC de Cisco há duas maneiras que você pode aproximar a construção ou o controlo de um perfil RF. Escolha **configuram > controladores > (endereço IP de Um ou Mais Servidores Cisco ICM NT do controlador) > 802.11 > RF perfila** a fim alcançar perfis para um controlador individual.

Isto indica todos os perfis RF atualmente atuais no controlador escolhido e permite que você faça mudanças às atribuições dos perfis ou do grupo AP. As mesmas limitações com respeito a um perfil que seja aplicado atualmente a um grupo AP são de fato como com o controlador GUI. Você tem que desabilitar a rede ou un-atribuir o perfil RF do grupo AP.



Quando você cria um perfil novo, os NC alertam-no escolher um molde existente. Se isto é a primeira vez está sendo alcançado, você está dirigido ao diálogo da criação do molde para um molde do controlador do 802.11.

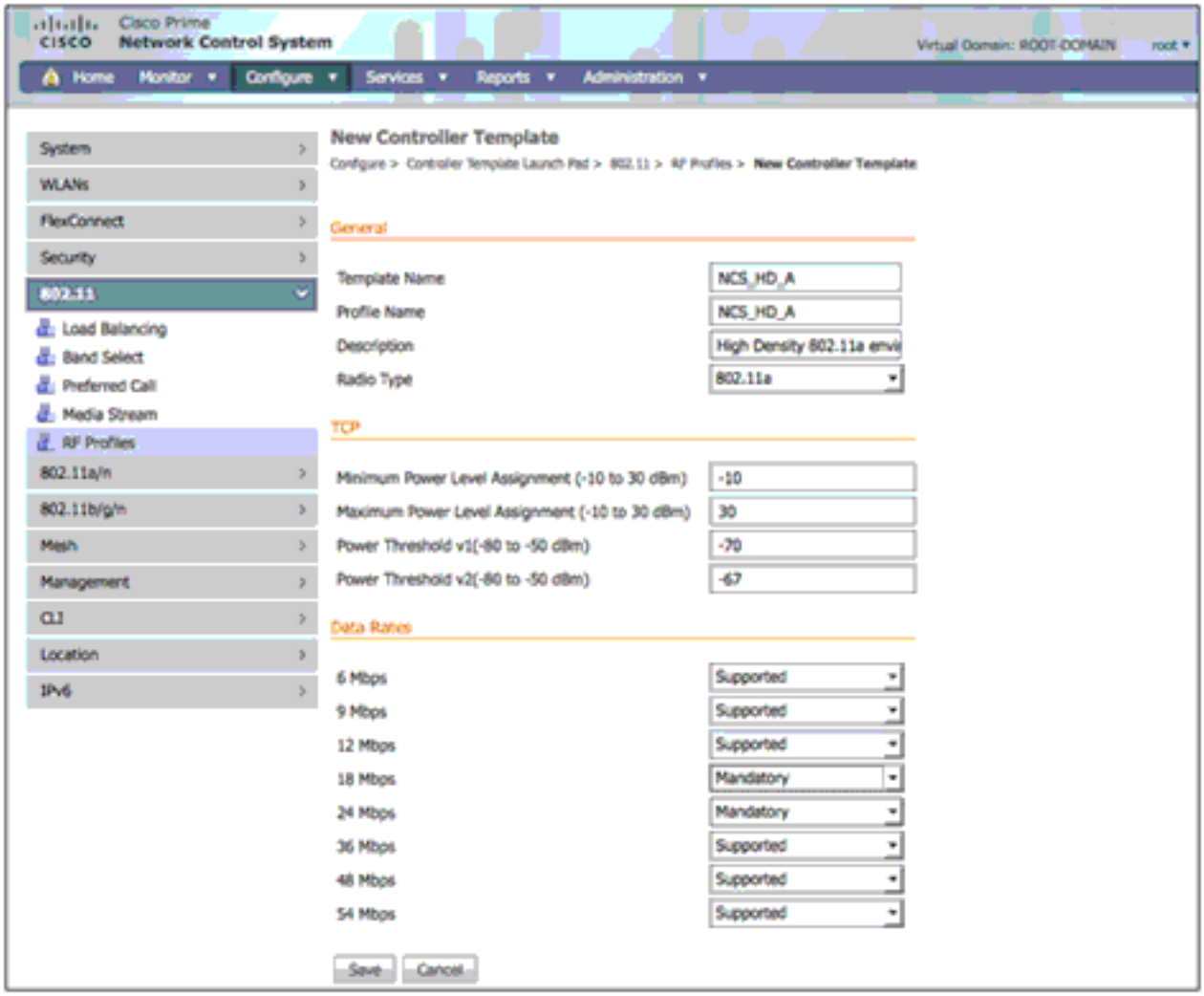


Escolha **configuram > base de lançamento do molde do controlador > 802.11 > perfis RF** a fim ir diretamente à base de lançamento do molde do controlador.

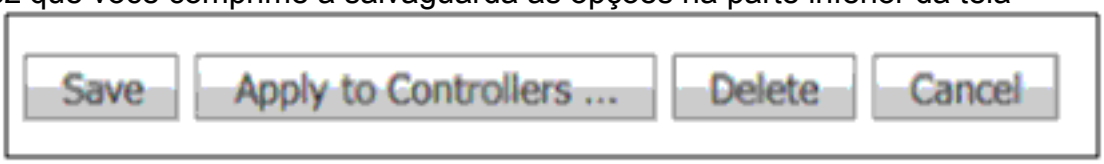
Em ambos os casos, um perfil novo RF é criado em NC com o uso de um molde. Este é um método preferido, desde que permite que o administrador leverage os trabalhos dos NC e aplique moldes e configurações a todos os ou aos grupos seletos controladores e reduza erros de configuração e más combinações.

Conclua estes passos:

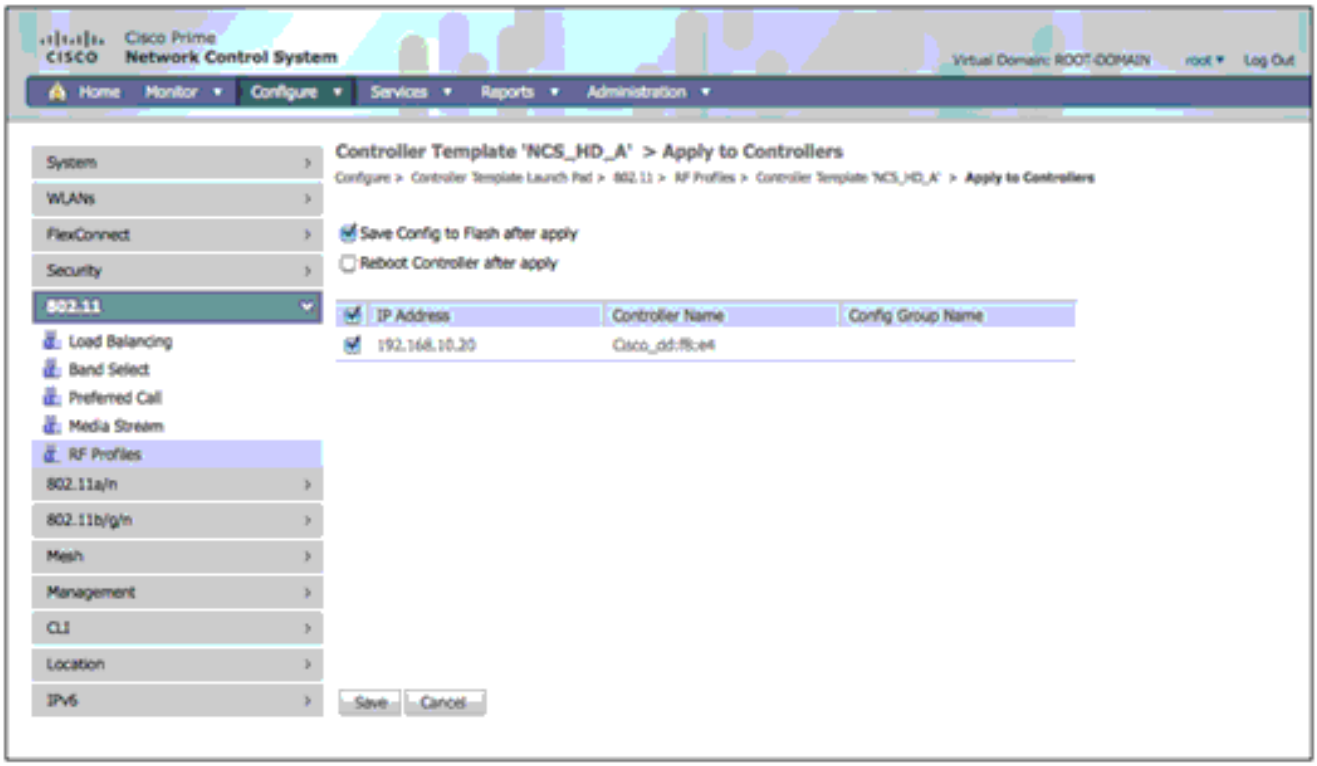
1. A fim criar um molde de perfil RF, escolha **novo**:



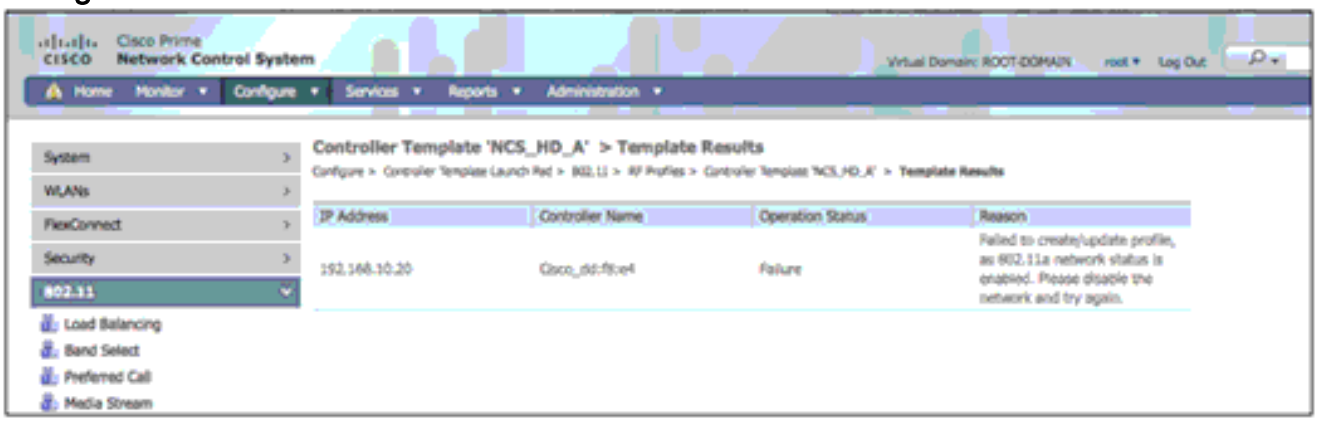
2. A configuração do molde/ajustes é quase idêntica com a adição de um nome de molde. Faça isto descritivo para o reconhecimento fácil no futuro. Mude ajustes como necessários ou exigidos e escolha a **salvaguarda**.**Nota:** Se você escolhe um valor de limiar para TPCv2 e não é o algoritmo escolhido TPC para o grupo RF, a seguir este valor está ignorado.**Nota:** Um ajuste simples a mudar para a validação é a potência do mínimo TPC. A potência mínima pode ser levantada se você escolhe um valor do dBm que seja mais do que o nível da potência atual atribuído por RRM. Isto ajuda a validar a operação dos perfis RF.
3. Uma vez que você comprime a salvaguarda as opções na parte inferior da tela



mudam Escolh a **aplicam-se aos controladores** e a caixa de diálogo do controlador parece indicar a lista de controladores controlados por este server NC.



4. Escolha a configuração da salvaguarda piscar, escolha o controlador que você deseja ter o perfil disponível sobre, e escolhe a **salvaguarda.**



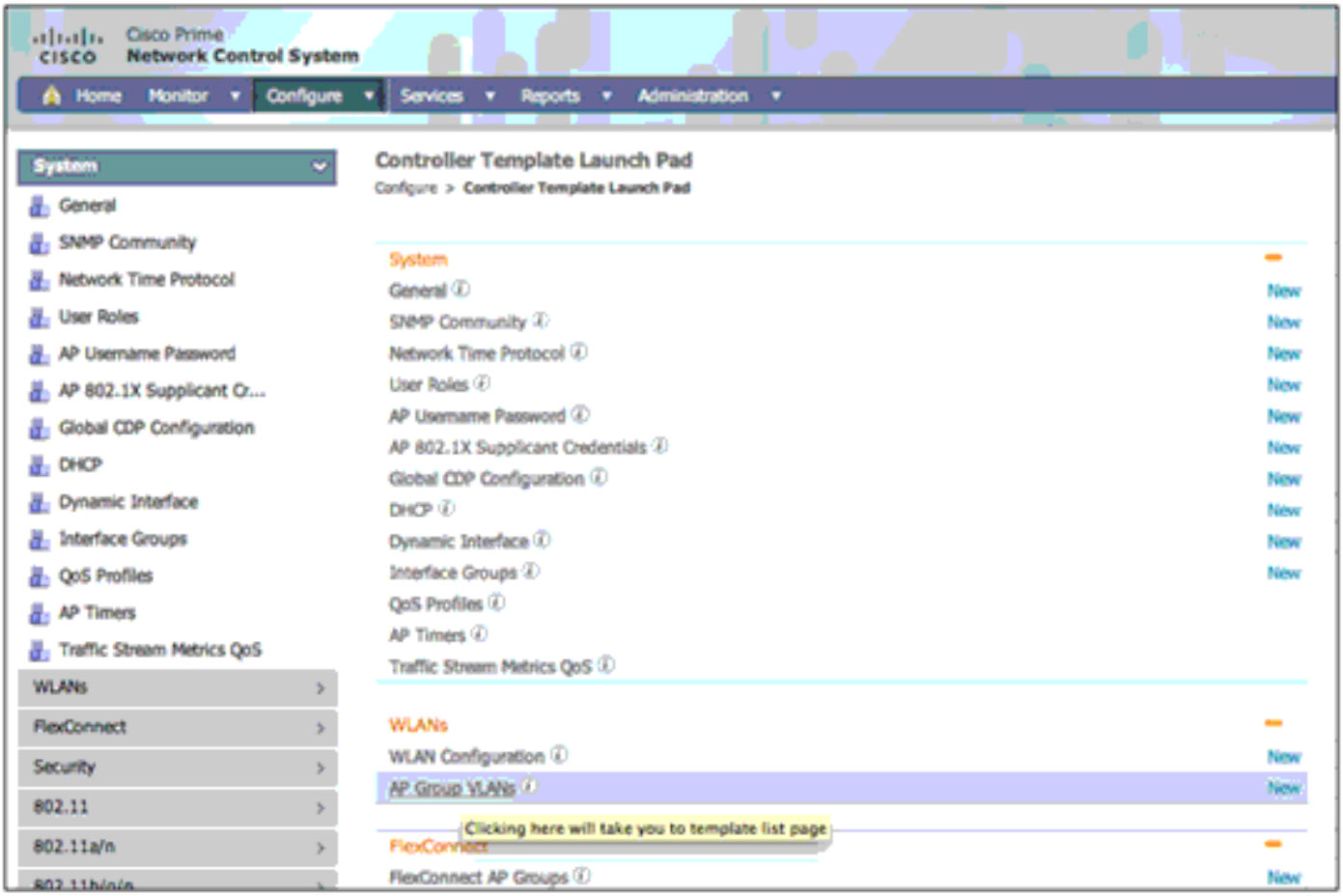
5. Agora em que você vê o RF perfila a tela, você pode ver o molde novo criado.

As etapas precedentes podem ser repetidas a fim criar como necessário e aplicar moldes adicionais, por exemplo, para 802.11b.

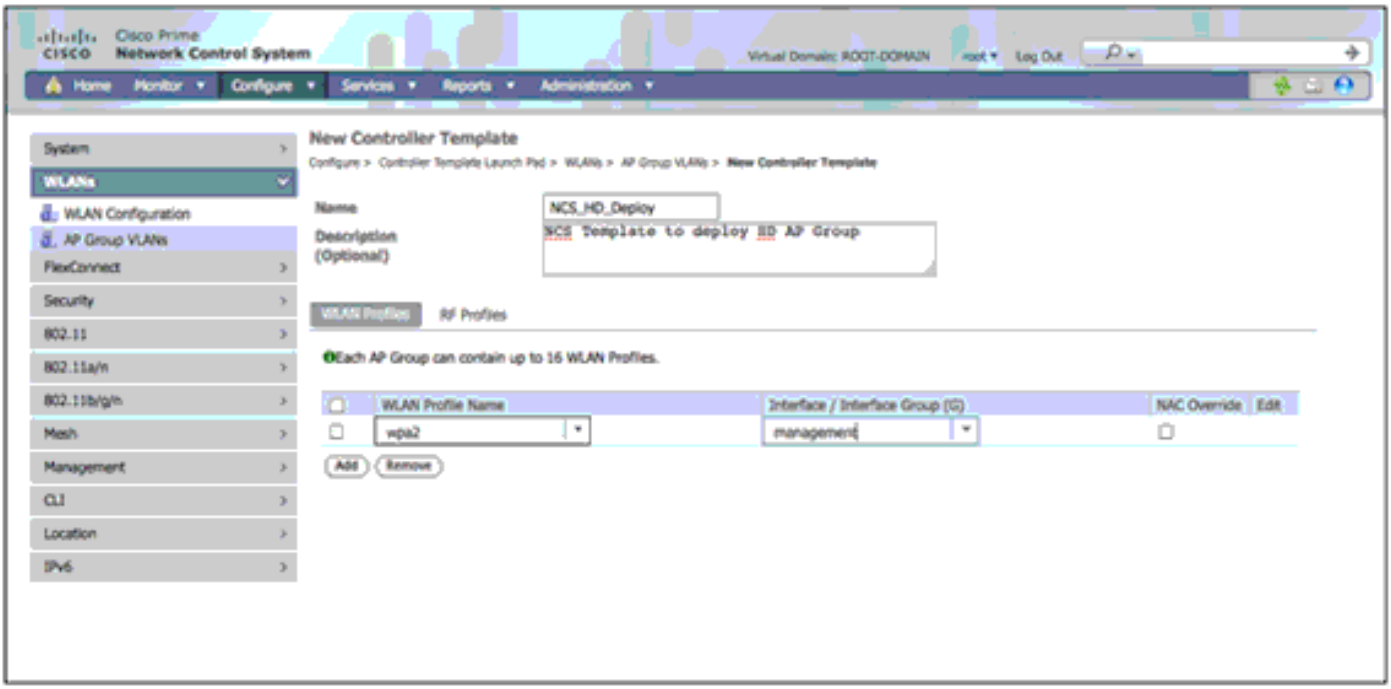
Aplique perfis RF aos grupos AP com NC

Como com a configuração WLC para perfis RF, os perfis recém-criados podem ser aplicados a um controlador com o uso de grupos que AP são atribuídos a. A fim fazer isto, ou salvar previamente o molde do grupo VLAN AP ou o molde recém-criado pode ser usado.

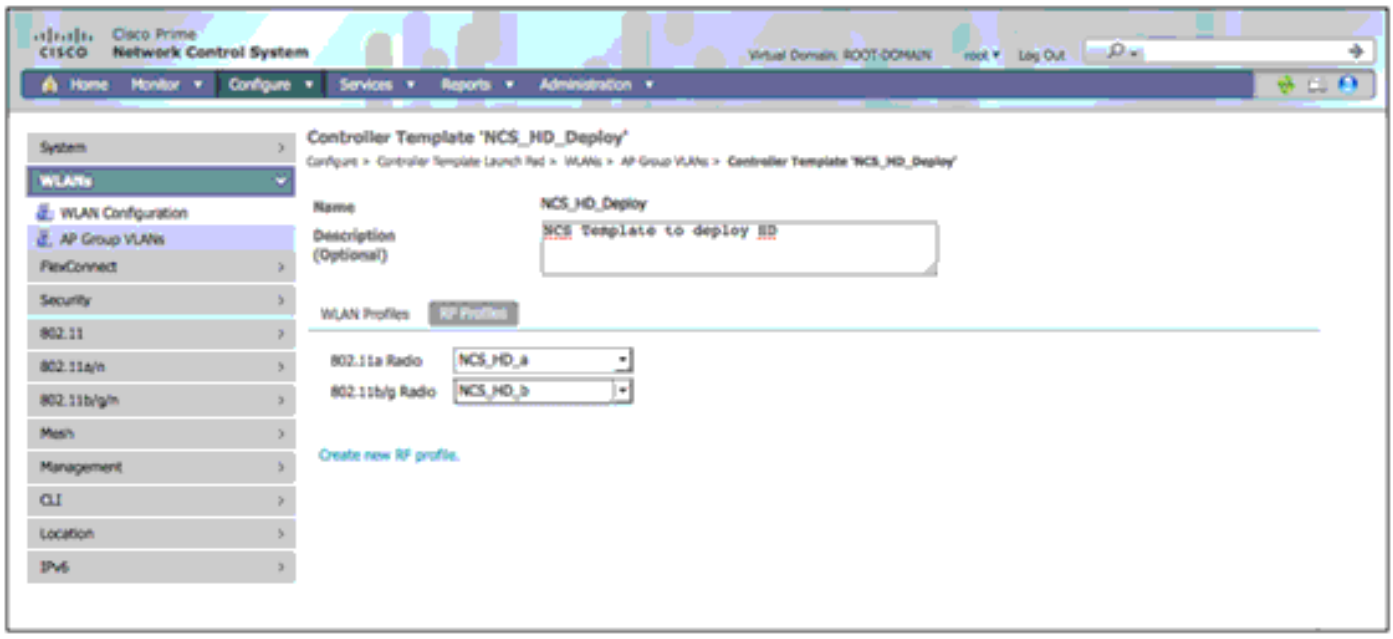
Escolha **configuram > base de lançamento do molde do controlador** e escolhem o **grupo VLAN AP**.



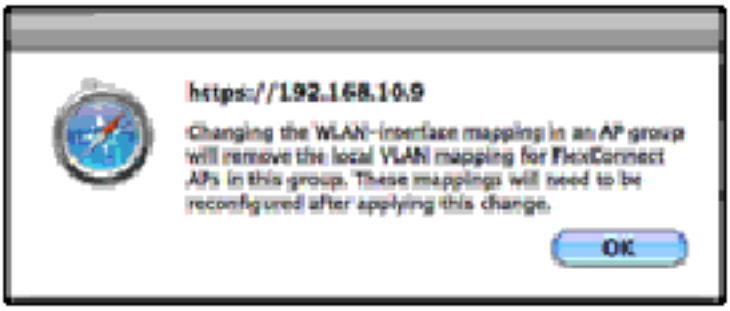
A fim criar um molde novo, escolha **novo** e preencha a informação requerida.



Escolha a aba dos **perfis RF** a fim adicionar perfis RF.



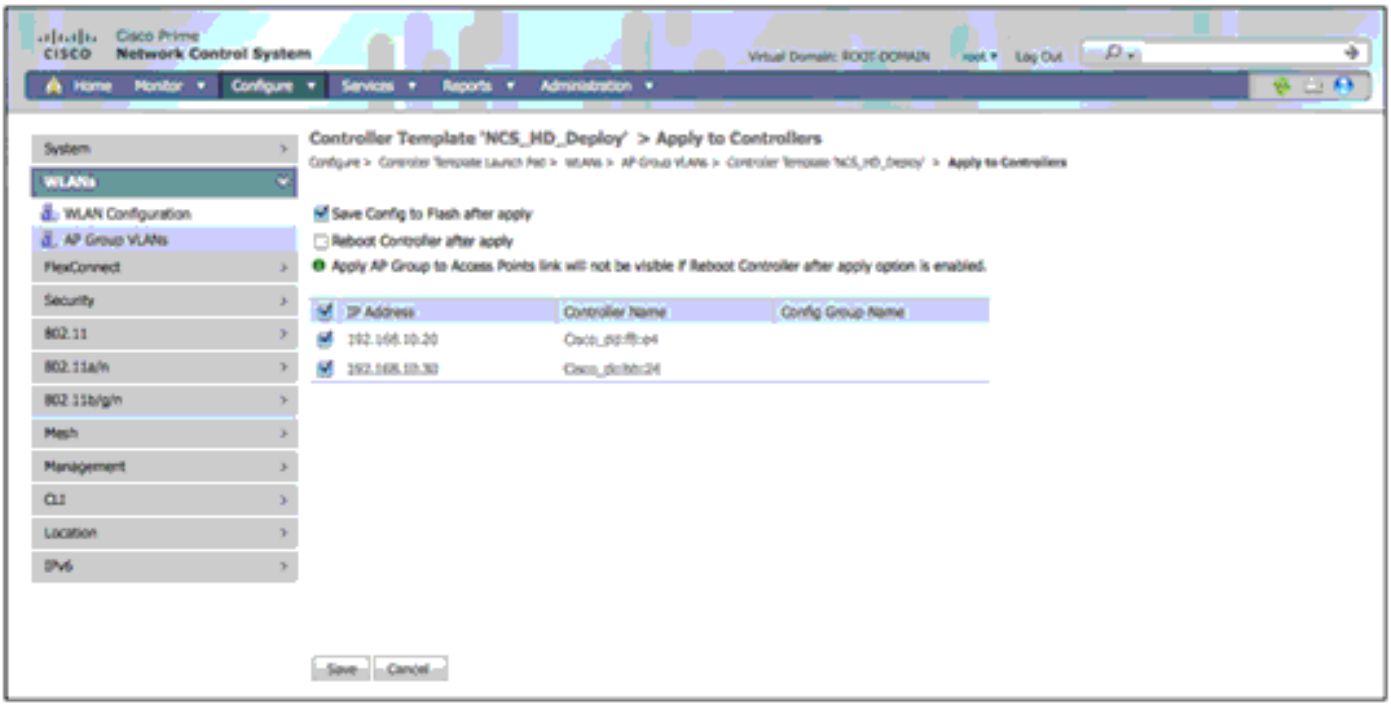
Se você salvar o molde, um mensagem de advertência aparece.



Como exposto no mensagem anterior, a mudança da relação que o WLAN atribuído usa interrompe os mapeamentos VLAN para FlexConnect AP aplicado neste grupo. Assegure-se de que a relação seja a mesma antes que você continue.

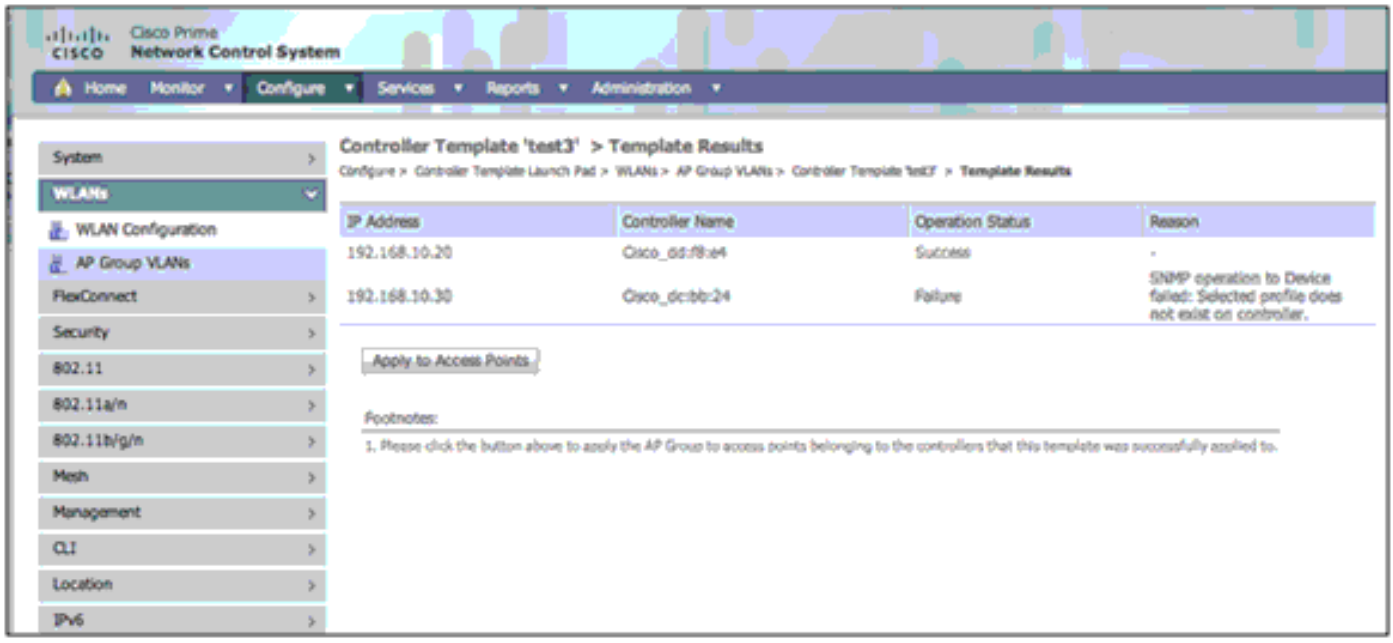
Uma vez que você escolhe **ESTÁ BEM**, o diálogo está substituído com a opção **para aplicar-se aos controladores**. Escolha esta opção.

Escolha os controladores a que o molde precisa de ser aplicado.



Os NC respondem com status operacional sobre se o molde esteve aplicado com sucesso aos controladores selecionados.

Se o molde não foi empurrado com sucesso, os NC fornecem uma mensagem que indique a razão para a falha. Neste exemplo, o perfil RF que é aplicado ao grupo não está atual em um dos controladores a que o molde era aplicado.

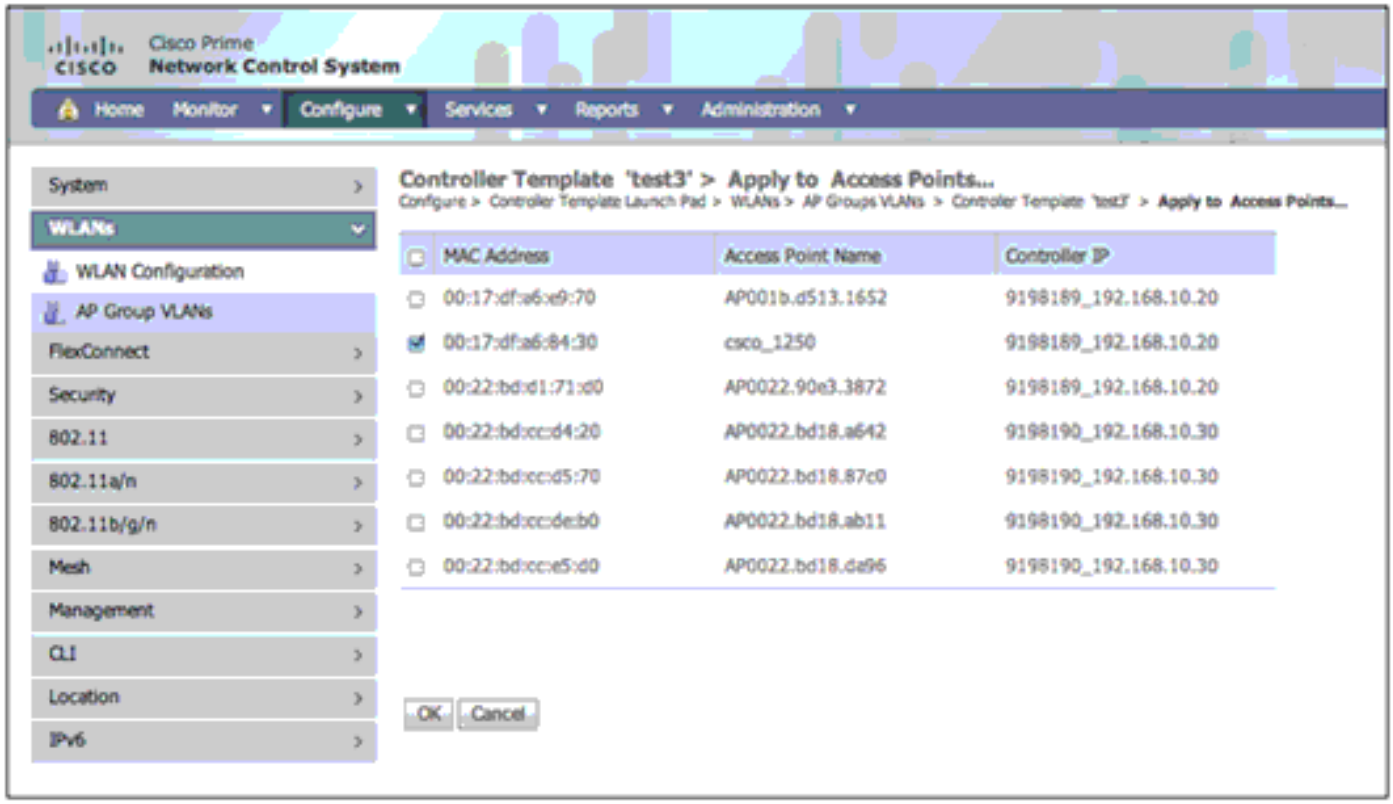


Aplique o perfil RF outra vez, especificamente a esse controlador e reaplique então o grupo AP a fim gerar uma mensagem bem sucedida.

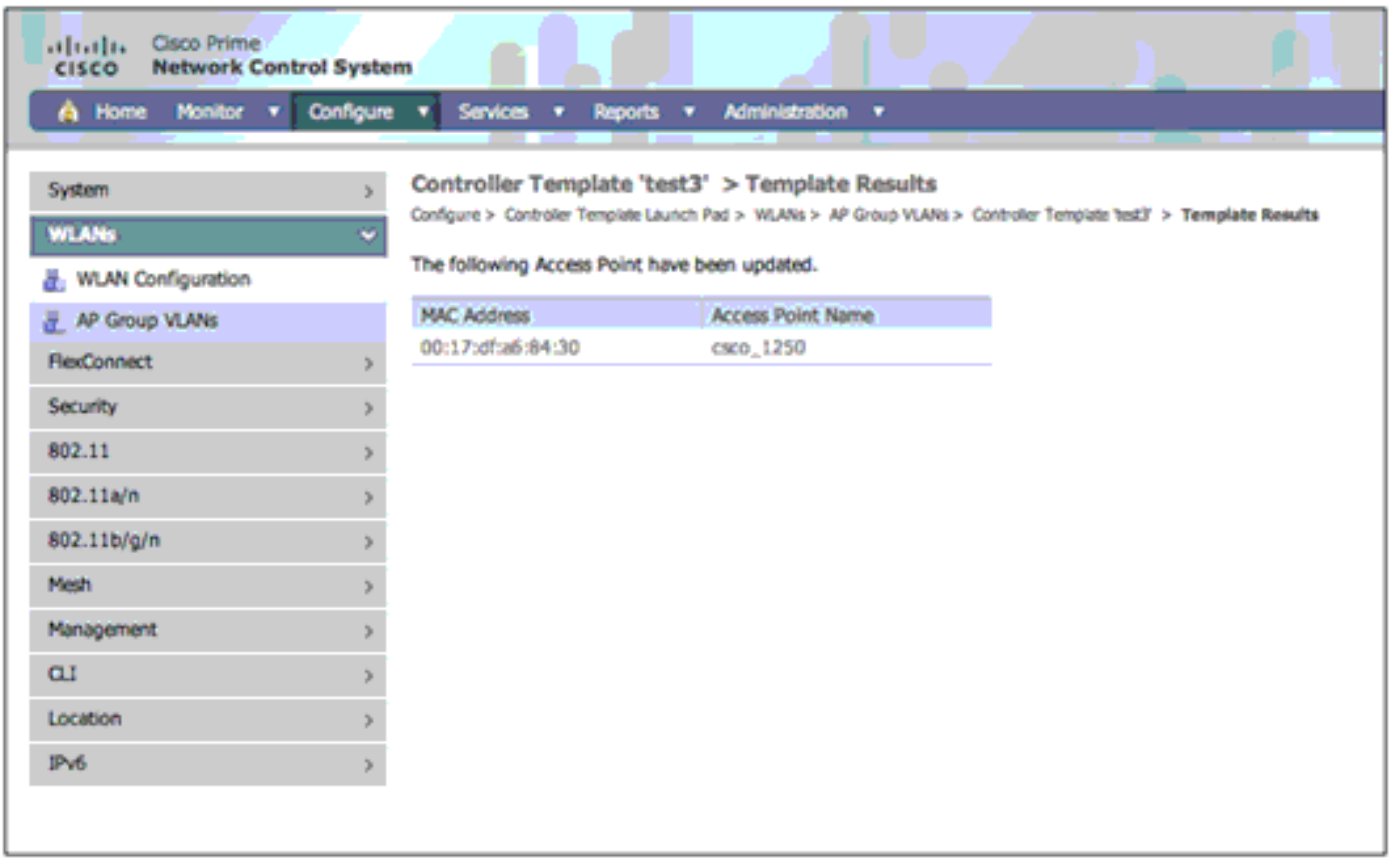
Uma vez que o grupo AP esteve distribuído com os perfis RF aplicados (escolha a **aplicação ao** botão dos **Access point**), simplesmente os Access point anexados aos controladores onde o grupo AP foi distribuído com sucesso estão disponíveis para selecionar de.

Nota: Até este ponto, nenhuma mudança real foi feita à infraestrutura RF, mas esta muda quando os AP são movidos no grupo que contêm perfis novos RF. Quando um AP é movido ou fora de um grupo AP, o AP recarrega a fim pegar a configuração nova.

Escolha os AP a fim adicionar ao grupo AP e escolher **ESTÁ BEM**. Um mensagem de advertência aparece.



Os NC indicam o estado da mudança.



Use NC às edições de Remediate

- CleanAir
- Troubleshooting do cliente
- ferramenta de auditoria
- painel da Segurança
- SPT

Use NC para aperfeiçoar o funcionamento da rede Wireless

- relatórios
- desempenho de rede Wireless (RRM)
- desempenho (largura de banda de WAN)

Painel

Os componentes do painel foram aumentados em NC 1.0 lá são um número de realces aos componentes do Home Page:

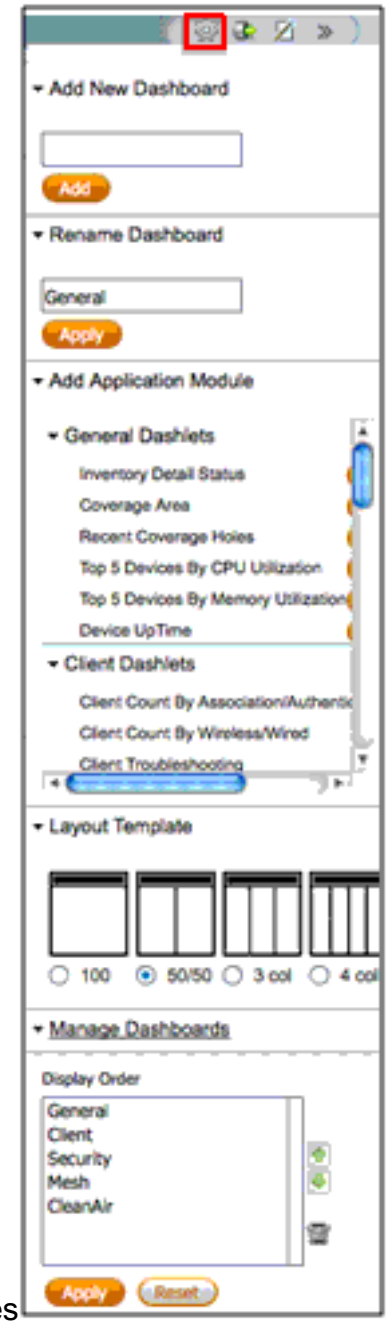
- integração prendida/wireless: os componentes agora igualmente indicam a informação prendida do cliente e do interruptor
- trabalhos componentes da personalização: o que pode ser personalizado, como personalizar
- os componentes individuais podem ser refrescados. A taxa de atualização pode ser

configurada individualmente também.

- facilidade da personalização do componente e do Home Page: toda a edição é terminada diretamente no Home Page (nenhuma necessidade de navegar para editar a página). Arraste e deixe cair para adicionar/componentes moventes
- trabalhos intuitivos: os hiperlinks componentes fornecem a facilidade da navegação, por exemplo distribuição do AUTH do cliente à página filtrada da lista do cliente

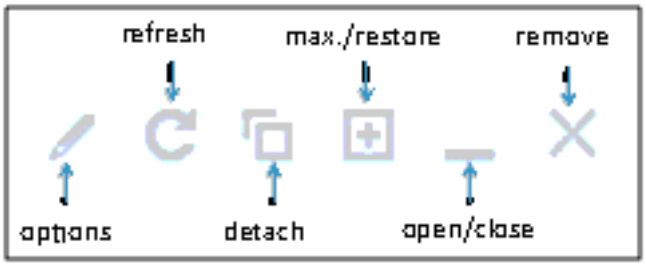
Estas são as personalizações principais do usuário para o painel:

- recursos arrastar e soltar do dashlet: os componentes podem ser rearranjados na página
- adicionar/suprimindo de painéis: adicionar/abas novas da supressão
- requisição do painel
- rebatismo do painel
- editando a disposição: pode especificar o número de colunas para dashlets, adicionar/que suprime de dashlets
- rebatizando dashlets
- múltiplas instâncias do dashlet: o usuário pode adicionar o mesmo dashlet e personalizar o índice em cada um
- disposição do painel dos configuráveis pelo usuário: número de colunas na página para

componentes 

Personalização de Dashlet:

- o manual refresca: permite que os usuários refresquem índices individuais do dashlet
- edite o nome do dashlet
- resize: minimize (reduza para intitular e barra de status), restaure (restaurações ao tamanho original), maximize (o dashlet ativo ocupa a área do painel)
- destaque: índice do dashlet destaque/redisplays na nova janela
- fim: remove o dashlet do painel. Pode ser adicionado outra vez através “adicionam da tela de Dashlet”
- opções múltiplas do indicador: gráfico ou tabela
- indicador visual a indicar se o dashlet esteve

personalizado. 

Única opinião prendido/clientes Wireless no dashlet

Há onze componentes do dashlet que fornecem a informação no prendido/clientes Wireless:

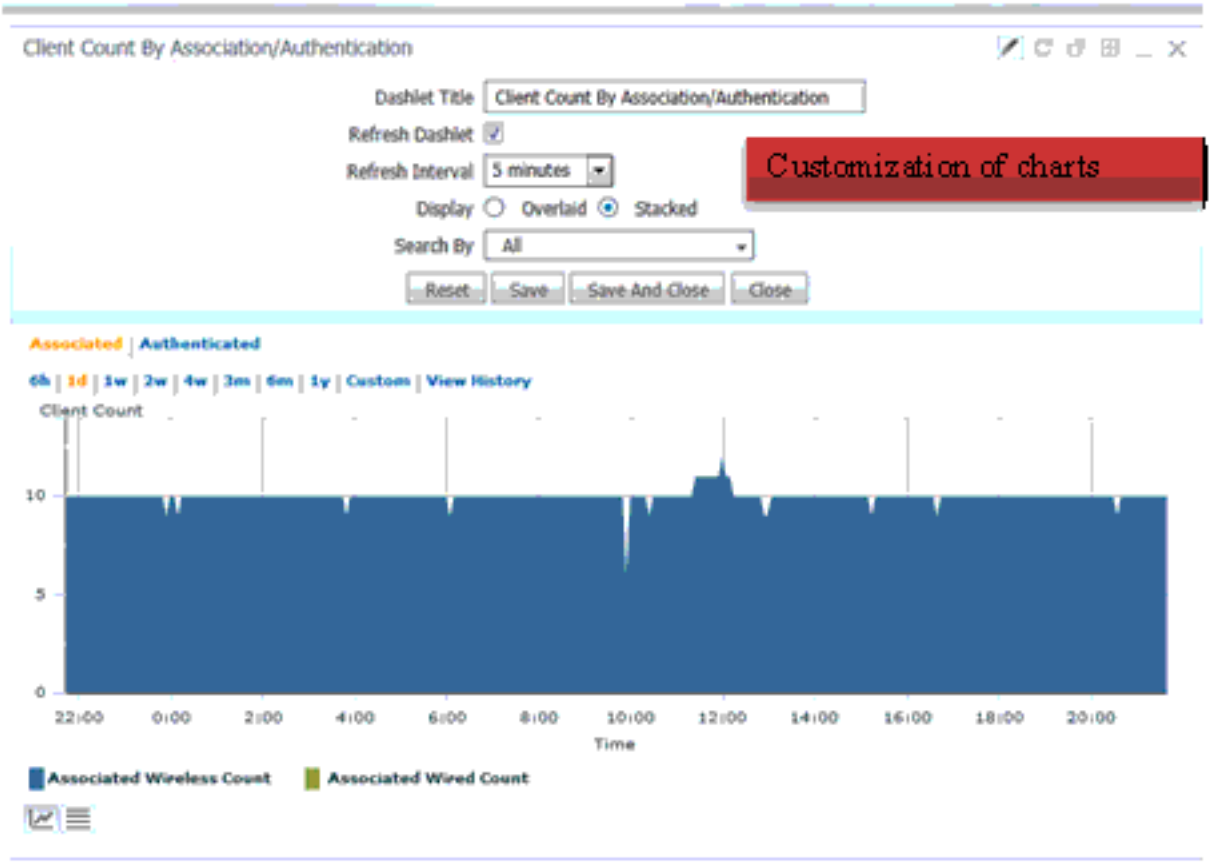
- Contagem do cliente pela associação/autenticação
- Contagem do cliente pelo Sem fio/prendida
- Tráfego do cliente
- Alarme e eventos do cliente sumários
- Tráfego do cliente
- Troubleshooting do cliente
- Estado da postura do cliente
- Estado do detalhe do inventário
- Uptime do dispositivo
- Dispositivos 5 superiores pela utilização CPU
- Dispositivos 5 superiores pela utilização de memória

Dashlets prendidos-somente

- Distribuição prendida da velocidade do cliente
- 5 Switch superiores pela contagem do cliente

Personalização de cartas de área

As cartas nos dashlets como a contagem do cliente pelo Sem fio/contagem prendido e do cliente pela autenticação da associação têm as cartas de área múltipla que dependem em cima da seleção da barra ad hoc do filtro das cartas que tem tudo/Sem fio/fio” e associado/autenticado respectivamente porque as opções na barra do filtro. As cartas de área consideradas podem ser cobertas (cruz das áreas múltiplas) ou ser empilhadas (as áreas múltiplas são empilhadas verticalmente – uma sobre a outro). A indicação de se está empilhada ou coberta é mostrada ao lado do título y-AXIS. A razão para os tipos diferentes de vistas (empilhadas ou cobertas) é dar ao usuário a melhor indicação do conjunto de dados que está sendo mostrado.

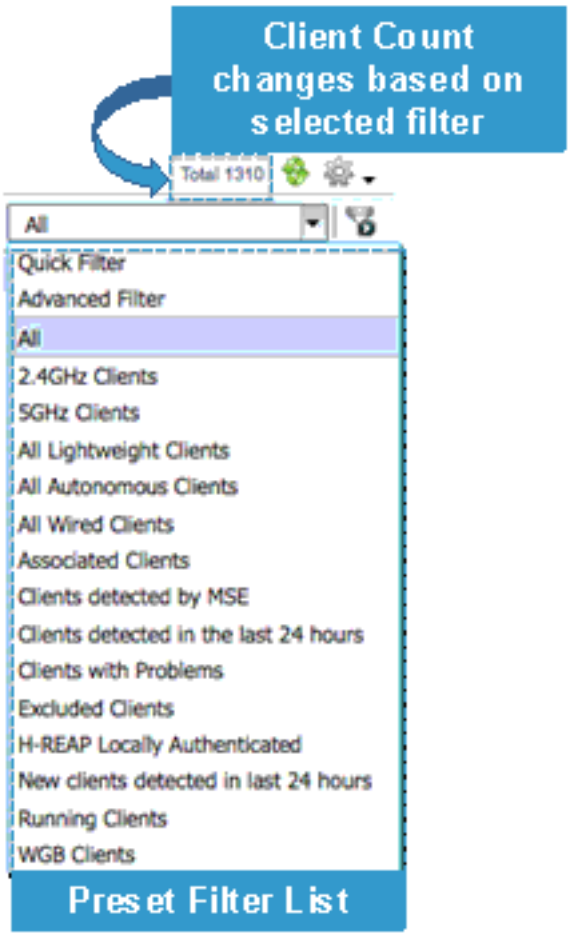


Monitorando clientes e usuários

Os NC fornecem a capacidade para monitorar prendido e clientes Wireless (**monitor > clientes e usuários**). Isto fornece uma opinião unificada todos os clientes na rede. Estes filtros estão disponíveis.

Durante a navegação a página à lista dos clientes e de usuários, todos os clientes associados é indicada à revelia. Há 14 filtros atuais que permitem que o usuário ver um subconjunto dos clientes. Os detalhes são fornecidos na tabela. Adicionalmente, há a opção para criar filtros feitos sob encomenda:

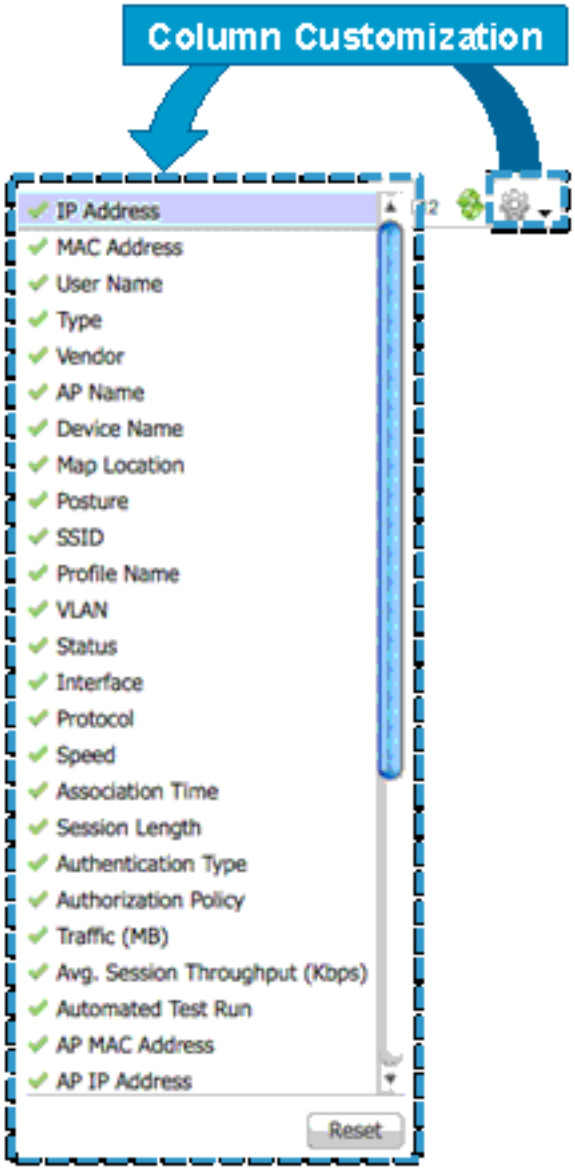
- Filtro rápido
- Filtro avançado



Filtros da lista do cliente	
Filtro	**Resultados**
Todos	Todo o incluir dos clientes inativo
clientes 2.4GHz	Todos os clientes Wireless ativos que usam a faixa do rádio 2.4 gigahertz
clientes 5GHz	Todos os clientes Wireless ativos que usam a faixa do rádio 5.0 gigahertz
Todos os clientes de pouco peso	Todos os clientes conectados aos AP de pouco peso
Todos os clientes autônomos	Todos os clientes conectados aos AP autônomos
Todos os clientes prendidos	Todos os clientes conectados diretamente para comutar controlado por NC
Clientes associados	Todos os clientes conectados apesar de se está autenticada ou não
Clientes detectados por MSE	Todos os clientes detectados incluir MSE prendido e por Sem fio
Clientes detectados em últimas 24 horas	Todos os clientes detectados em últimas 24 horas

Clientes com problemas	Os clientes que são associados, mas não terminaram a política.
Clientes excluídos	Todos os clientes Wireless de pouco peso que estão sendo excluídos pelo controlador
H-REAP autenticado localmente	Os clientes conectaram a H-REAP AP e autenticaram localmente
Clientes novos detectados em últimas 24 horas	Todos os clientes novos detectados em últimas 24 horas
Clientes running	Clientes que terminaram todas as políticas do grupo e estão no estado de execução.
Clientes WGB	Todos os clientes WGB

As colunas na tabela da lista do cliente podem ser personalizadas diretamente nesta página.



As colunas na tabela da lista do cliente podem ser personalizadas diretamente página na lista dos **clientes e de usuários**. Selecione ou colunas do unselect a fim indicar imediatamente ou esconder

a coluna.

Opte pelo grupo de colunas indicadas e sua ordem pode ser restaurada ao valor padrão através do **botão reset**.

Em ordem o requisite novamente colunas, arraste a coluna diretamente na página e mova-a para a ordem/lugar desejados.

Cliente e página de usuário: Detalhes da coluna	
Atributo	**Comentários**
Endereço IP	Endereço IP cliente
Endereço MAC	Endereço MAC cliente
Username	Username baseado na autenticação do 802.1x. O desconhecido é indicado para o cliente conectado sem um username
Tipo	O ícone representa um peso leve, um cliente autônomo ou prendido.
Vendedor	Vendedor do dispositivo derivado do OUI
Nome AP	Sem fio somente
Nome de dispositivo	Nome de dispositivo da autenticação de rede, por exemplo WLC, interruptor.
Lugar do mapa	Lugar do mapa do dispositivo conectado.
Postura	O estado o mais atrasado da postura do cliente
SSID	Sem fio somente
Nome de perfil	Sem fio somente
VLAN	O dispositivo VLAN está ligada
Status	Estado do cliente atual
Interface	A relação do controlador (Sem fio) ou a interface de switch (prendida) esse cliente são conectam a.
Protocolo	802.11 - Sem fio 802.3 - prendido.
Velocidade	Velocidade da porta Ethernet - prendida somente. Indicador “N/A” para o Sem fio
Tempo da associação	Últimas horas inicial da associação AP, Sem fio somente
Comprimento da sessão	Comprimento da sessão
Tipo de autenticação	WPA, WPA2, 802.1x, etc.
Tipo de autorização	Tipo de autorização prendido do ISE

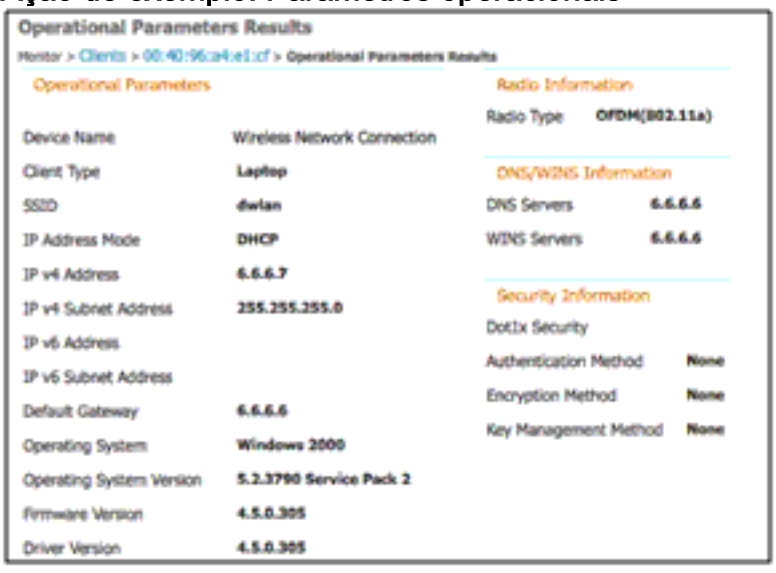
Tráfego (MB)	Trafique (transmitido/recebido) nesta sessão no MB
Taxa de transferência média da sessão (kbps)	Taxa de transferência média da sessão nos kbps
Execução de teste automatizada	Indica se o cliente reage do auto modo de teste
MAC address AP	Sem fio somente
Endereço IP de Um ou Mais Servidores Cisco ICM NT AP	Sem fio somente
Controlador da âncora	Sem fio de pouco peso somente
Executando	O cliente terminou todas as políticas do grupo.
CCX	Sem fio de pouco peso somente
Nome de host do cliente	Prendido e Sem fio. Resultado da consulta reversa DNS.
Endereço IP de Um ou Mais Servidores Cisco ICM NT do dispositivo	Endereço IP de Um ou Mais Servidores Cisco ICM NT do dispositivo conectado (WLC, interruptor ou aIOS AP).
Porta	Switchport no WLC
E2E	Sem fio de pouco peso somente.
Cifra da criptografia	Sem fio somente
MSE	Server MSE que controla este cliente
RSSI	Sem fio somente
SNR	Sem fio somente
ID de sessão	Auditoria-sessão-ID usado no ISE e no interruptor
Tempo de sessão	Horas inicial da sessão por horas inicial da sessão da sessão ativa – tempo do fim da sessão para a sessão inativa
Nome do vendedor	Nome do vendedor derivado do OUI

A barra de ferramentas o cliente/lista de usuários fornece um grupo de ferramentas que podem ser invocadas em clientes selecionados (uns ou vários).

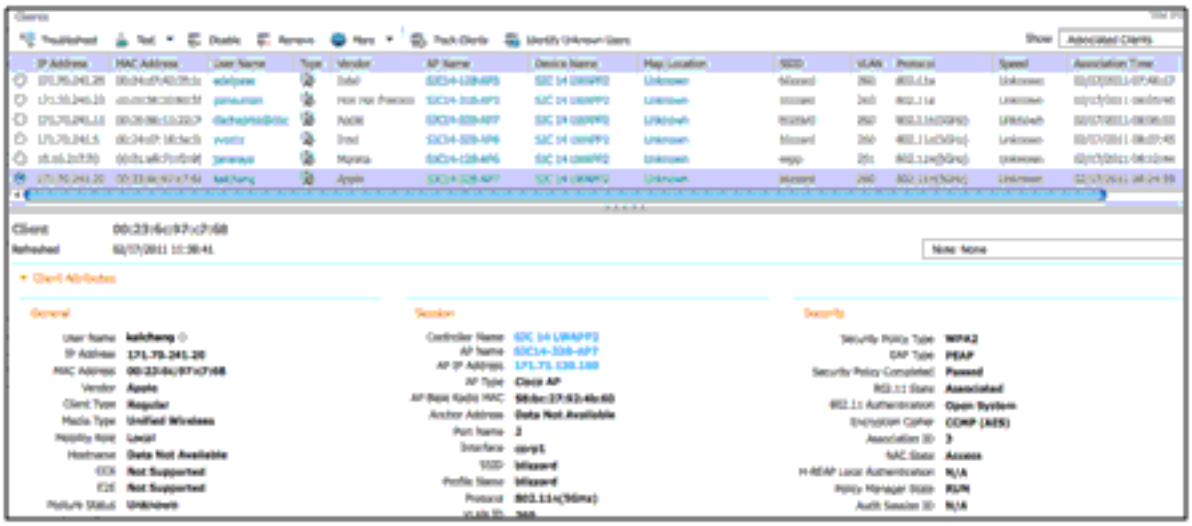
Monitor > clientes e usuários: Comandos suportados	
Comando	**Tipo de cliente**
Troubleshooting	Todos
Teste o menu	

Ligue o teste	Sem fio de pouco peso somente
Medidas de rádio	Sem fio de pouco peso somente
Estatísticas V5	Sem fio de pouco peso CCX v5 somente
Parâmetros operacionais	Sem fio de pouco peso CCX v5 somente
Disable	Sem fio de pouco peso somente
Remova	Sem fio de pouco peso somente
Mais menu	
Perfis	Peso leve (CCXv5)
Vagueie a razão	Sem fio de pouco peso somente
Mapa recente	Sem fio de pouco peso somente
Mapa atual	Sem fio de pouco peso somente
Sessões	Todos
Detectando AP	Sem fio de pouco peso somente
História do lugar	Sem fio de pouco peso somente
Permita o modo do espelho	Sem fio de pouco peso somente
Medidor da Voz	Sem fio de pouco peso somente
Clientes da trilha	Sem fio de pouco peso somente
Identifique clientes desconhecidos	Todos

Ação de exemplo: Parâmetros operacionais



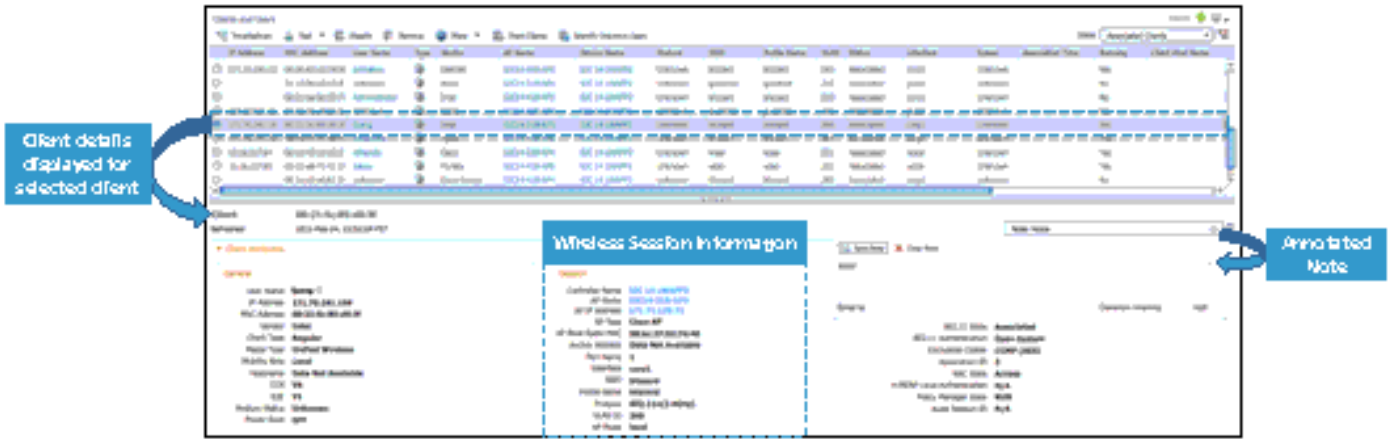
O botão de rádio sobre ao lado esquerdo escolhe um cliente específico indicar detalhes do cliente nesta lista do cliente.



cliente Wireless de pouco peso

cliente prendido

Neste tiro de tela, o cliente na parte inferior da lista é um cliente Wireless do peso leve (tipo: Sem fio de pouco peso).



O exemplo é para o cliente prendido.

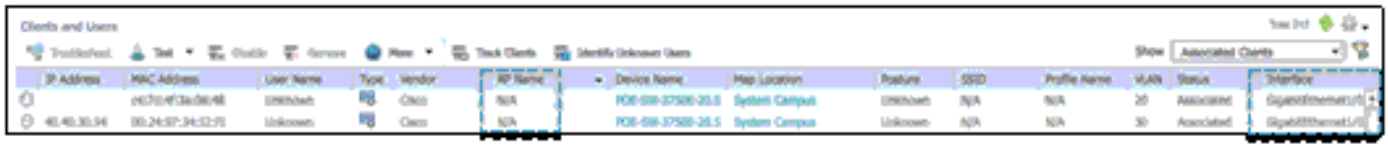
Troubleshooting prendido/cliente Wireless

Na monitoração prendida e wireless NC 1.0, e no Troubleshooting foi integrado com serviços da identidade. A integração entre o Gerenciamento prendido/rede Wireless foi conseguida através de três elementos de rede:

- Controladores de LAN do Cisco Wireless (WLC)
- Recursos de segurança do interruptor do Cisco catalyst: AAA, RAIO, 802.1x e autenticação de MAC, armadilhas da notificação MAC (clientes da NON-identidade), Syslog (clientes da identidade somente)
- Cisco Identity Services Engine (ISE)

Todos os clientes – prendidos e Sem fio – são indicados na página dos clientes e dos usuários (**monitor > clientes e usuários**).

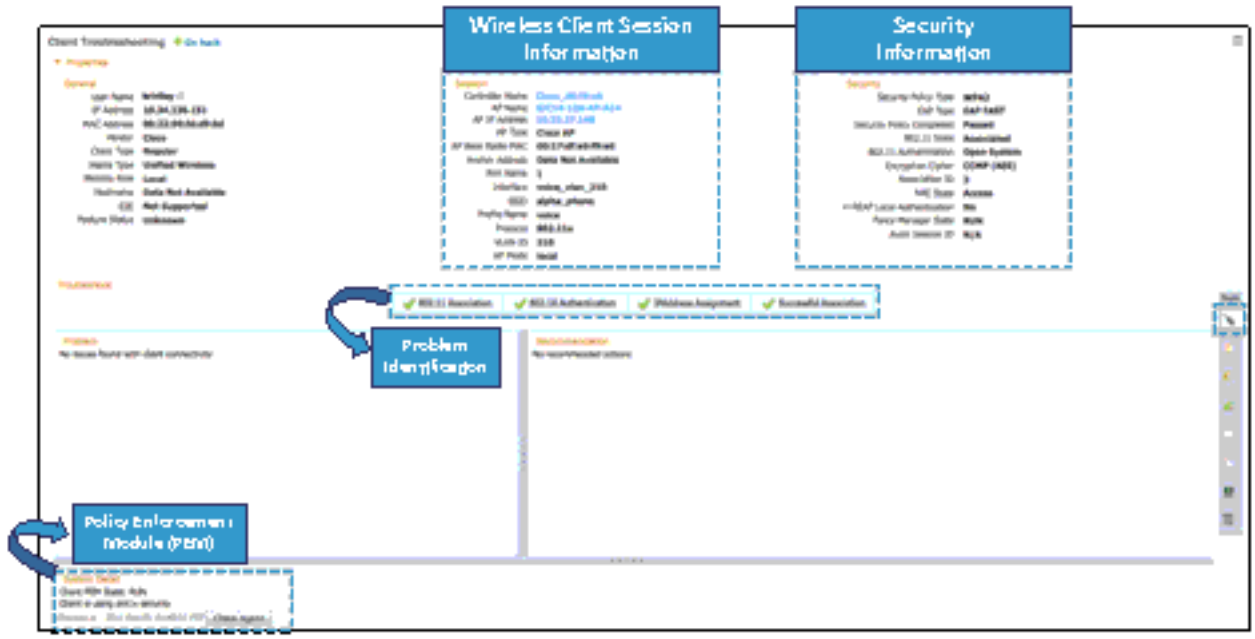
O nome prendido do indicador **AP dos** clientes como a informação de porta de switch *N/A.* é fornecido nas **relações**.



Troubleshooting do cliente Wireless

A fim lançar a ferramenta de Troubleshooting do cliente, clique sobre o botão de rádio à esquerda do artigo da lista do cliente. Uma vez que o cliente é selecionado, clique sobre o ícone do **Troubleshooting na** barra de ferramentas.

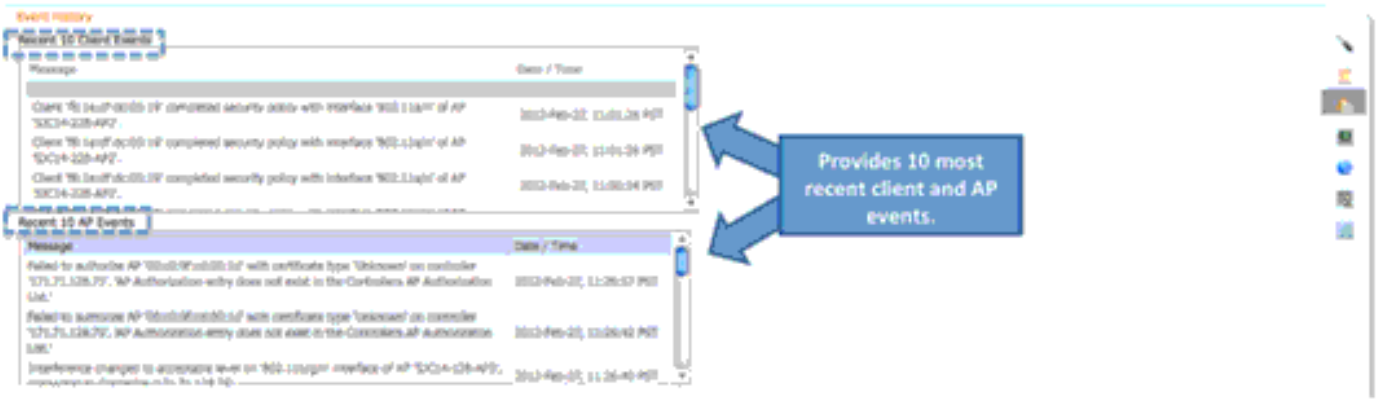
O indicador é indicado para o cliente.



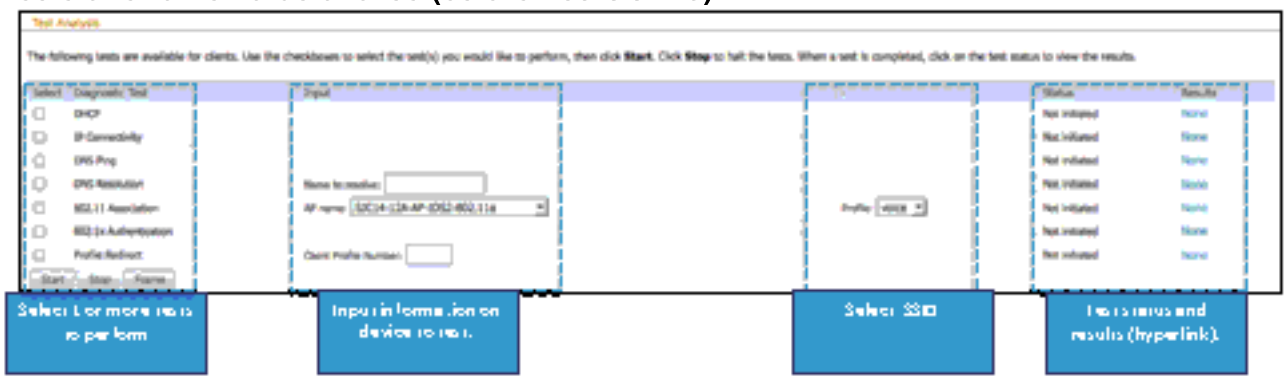
Os mensagens de registro podem ser recuperados do controlador com o uso da ferramenta de análise do log.

Refira o módulo do reforço de política (PEM) para obter mais informações sobre do estado PEM.

A ferramenta da história do evento fornece o usuário os mensagens de evento do cliente e do AP.



Teste a ferramenta de análise (os clientes CCXv5)



Troubleshooting prendido do cliente

Os NC 1.0 fornecem o gerenciamento integrado do prendido e dispositivos Wireless/clientes. Um dos recursos principais em NC 1.0 é de monitoração e de pesquisa de defeitos para prendido e clientes Wireless. O SNMP é usado para descobrir clientes e recolher dados do cliente. O ISE é votado periodicamente para recolher estatísticas do cliente e outros atributos para povoar

componentes e relatórios relacionados do painel.

Se o ISE é adicionado aos sistemas e os dispositivos lhe estão autenticando, o cliente detalha a página indica os detalhes adicionais etiquetados como a Segurança.

A fim navegar à página de Troubleshooting do cliente, clique sobre o ícone do **Troubleshooting no** menu das ferramentas na parte superior da página.

Isto toma o usuário à página mostrada no screen shot. Neste exemplo, o dispositivo do cliente tem a Conectividade do link, mas a autenticação de MAC falhada.

No lado direito da tela é uma barra de ferramentas com estes artigos toda relacionados à pesquisa de defeitos:

- Ferramenta de Troubleshooting do cliente
- Análise do log
- História do evento
- História ciente do contexto

A história do evento fornece as mensagens relativas aos eventos da Conectividade para este cliente. Neste exemplo, o cliente não são autenticados com sucesso. A data/hora é fornecida de ajudar ao administrador de rede em pesquisar defeitos este cliente.

O ISE fornece registros da autenticação aos NC através do RESTO API. O administrador de rede pode escolher o período de tempo para recuperar registros da autenticação do ISE. Neste

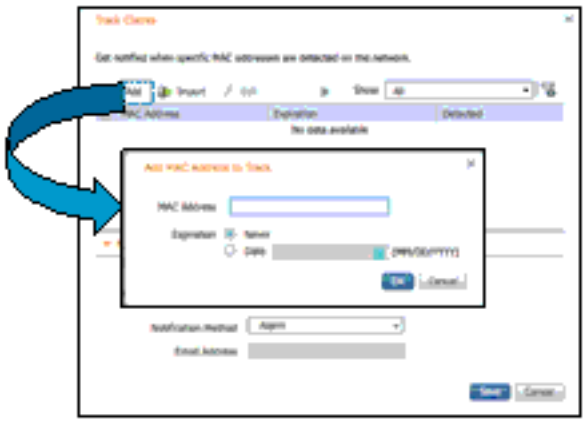
exemplo, o registro da autenticação indica que o usuário não esteve encontrado no base de dados ISE.

Características RF/Wireless

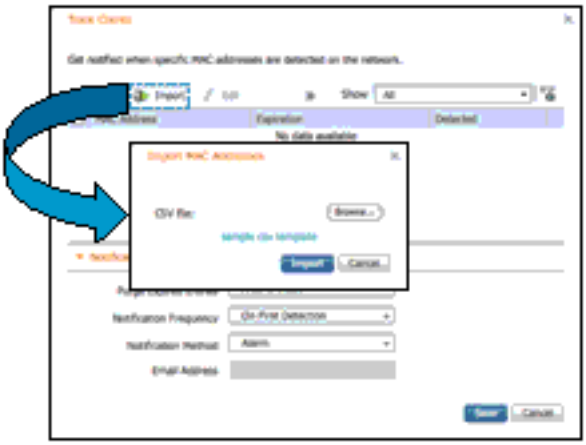
Clientes da trilha

Esta característica permite que um administrador de rede siga clientes específicos e seja notificado quando estes clientes conectam à rede. Esta característica é permitida da página do monitor > dos usuários e dos clientes.

Para seguir o único cliente, clique o **botão Add** e um secundário-indicador aparece onde o usuário pode incorporar o MAC address do cliente junto com a expiração de seguimento (nunca ou data final especificada).



Se o usuário quer seguir clientes múltiplos, a lista do cliente pode ser importada. O indicador resultante permite o usuário à lista de importação de endereços MAC de cliente através do arquivo CSV.



Um arquivo CSV da amostra pode ser transferido que forneça o formato de dados.

```
# MACAddress, Expiration: Never/Date in MM/DD/YYYY format
00:40:96:b6:02:cc,10/07/2010
00:02:8a:a2:2e:60,Never
```

Ajustes da notificação

Há três opções para notificações:

1. Entradas expiradas removidas — o usuário pode ajustar a duração para manter clientes seguidos no base de dados NC. Os clientes podem ser removidos:após 1 semanaapós 2 semanasapós 1 mêsapós 2 mesesapós os meses 6mantido indefinidamente
2. Frequência da notificação — o usuário pode especificar quando os NC enviam a notificação do cliente seguido:na primeira detecçãoem cada detecção
3. Método de notificação — o usuário pode especificar para que o evento de cliente seguido gerencia o alarme ou envie o email.

Indicando clientes seguidos

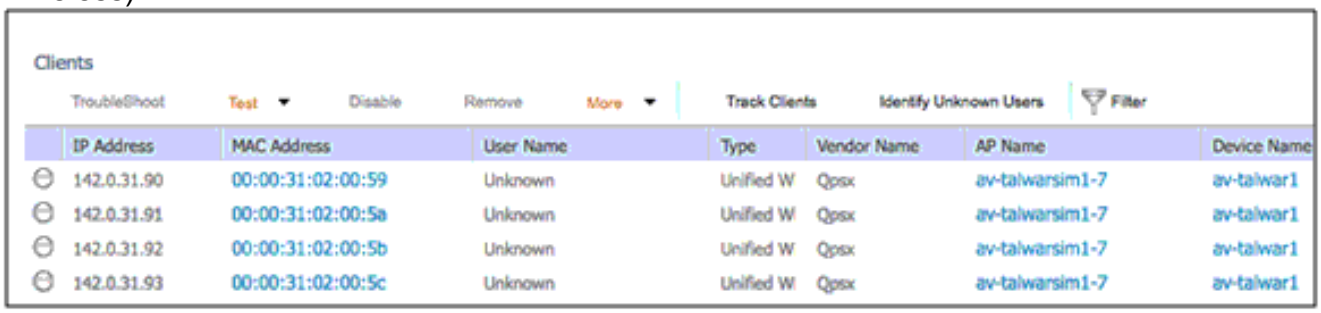
Depois que a informação sobre o usuário seguida foi incorporada, o indicador seguido dos clientes permite que o usuário ver o estado de clientes seguidos existentes.

Usuário desconhecido - identificação

Não todos os usuários/dispositivos são autenticados através do 802.1x (por exemplo impressoras). Neste evento, a rede administra tem a opção para atribuir um nome ao dispositivo.

Se um dispositivo do cliente é autenticado à rede através do AUTH da Web, o WCS não pode ter a informação de nome de usuário para esse cliente. Nesta encenação, os clientes podem querer ter os nomes de usuário traçados aos clientes, mesmo se estão usando o AUTH da Web.

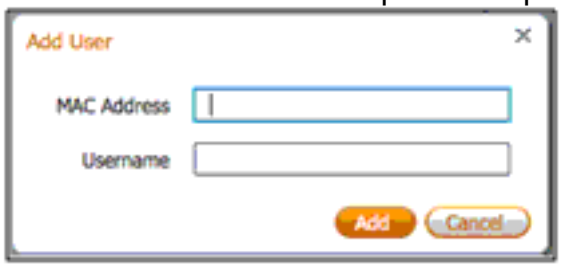
1. Escolha o **monitor > os clientes**.Os clientes wireless e prendidos são indicados. Como descrito anteriormente, uma barra de ferramentas é ficada situada na lista precedente de clientes que permite que o usuário invoque um número de ações:pesquise defeitosteste (teste do link, medida de rádio, estatísticas CCXv5, parâmetros de operação)disableremova (dissociar o cliente
   Wireless)



2. Clique o ícone dos **usuários desconhecidos da identificação na** barra de ferramentas.

   Isto resulta com uma janela pop-up.

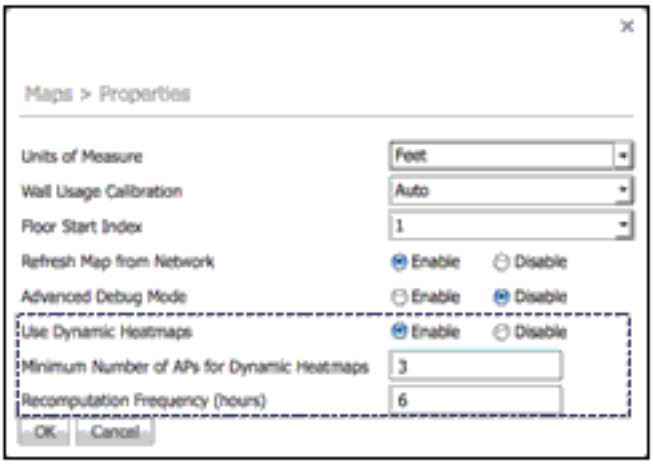
3. O clique **adiciona** a fim inscrever detalhes do cliente. 

O MAC address individual e o username correspondente podem ser adicionados. 

Uma vez que um cliente e um MAC address foram adicionados, o WCS usa esta tabela para a consulta do cliente baseada no MAC address de harmonização.

Mapas do calor do tempo real

Um dos novos recursos em NC 1.0, é a opção para indicar mapas do calor do tempo real. Iss está habilitado por padrão. Escolha o **monitor > os mapas > as propriedades** a fim navegar aos ajustes.



Monitorando o Switches do Cisco catalyst usando NC

A informação prendida do inventário é determinada por estes métodos:

- Descoberta prendida do cliente através do SNMP traps, do polling snmp e dos mensagens do syslog do Switches
- ISE API northbound para a informação adicional, tal como a postura, perfilador, contabilidade, e assim por diante

Os NC fornecem a paridade de recurso o WCS 7.x para a monitoração do cliente e o relatório em todos os clientes (prendidos e Sem fio). Adicionalmente, Troubleshooting dos cruz-lançamentos ISE NC para clientes prendidos. Um nível mais adicional da integração ISE é através do cruz-lançamento de relatórios ISE com os dados não contidos no WCS.

Esta informação do interruptor é fornecida nos NC:

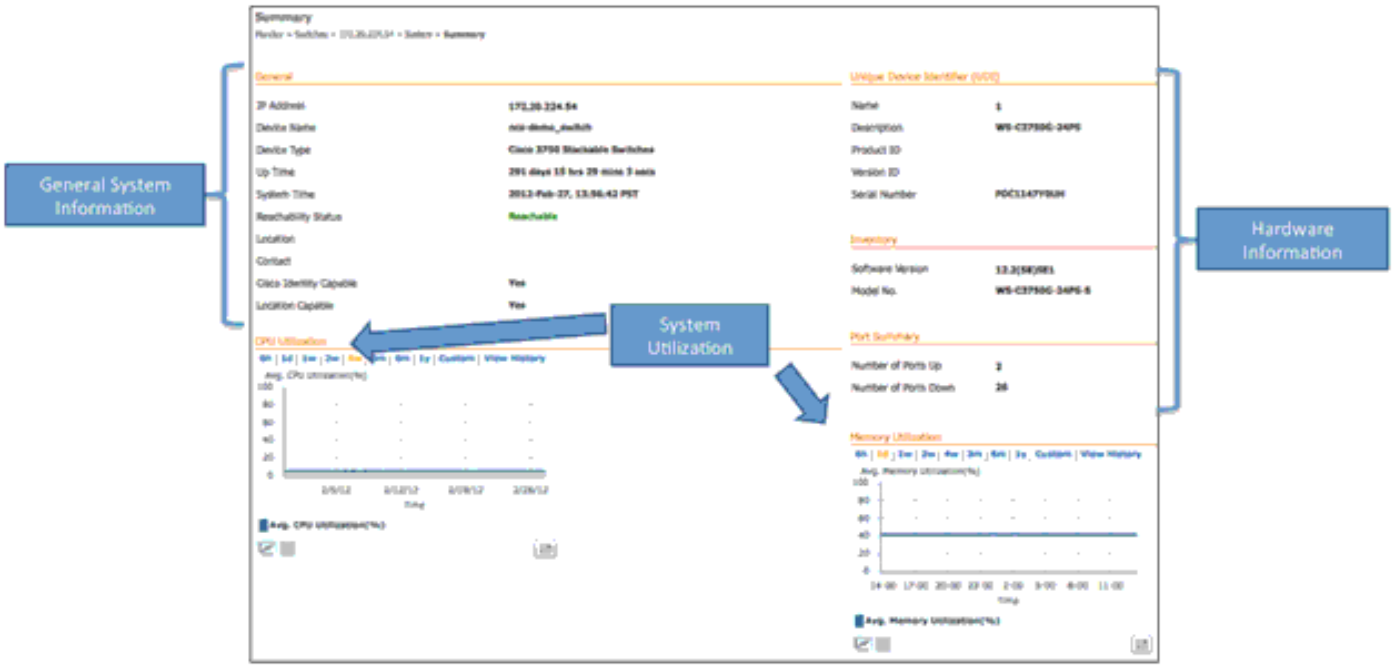
- Ativos físicos, por exemplo, chassi, módulos, porta, e fonte de alimentação da entidade MIB
- Dispositivo flash/separação/arquivos
- Imagem instalada do software
- Interface de Ethernet
- Interface IP
- Interface de VLAN
- VLAN e VTP
- EtherChannel
- STP
- StackWise (apoiada somente em Cisco Catalyst 3750 Switch)

O monitor > o interruptor indicam esta informação do interruptor:

- Endereço IP
- Nome de dispositivo: hostname como dado na configuração do IOS do interruptor
- Tipo de dispositivo: modelo de switch

- Alcançabilidade: Conectividade de SNMP
- Contagem do cliente: número de clientes conectados diretamente ao interruptor

O endereço IP de Um ou Mais Servidores Cisco ICM NT indicado é um hiperlink, e clicar nele toma o usuário **para configurar > Switch Ethernet > (endereço IP de Um ou Mais Servidores Cisco ICM NT) >** tela **sumária**.

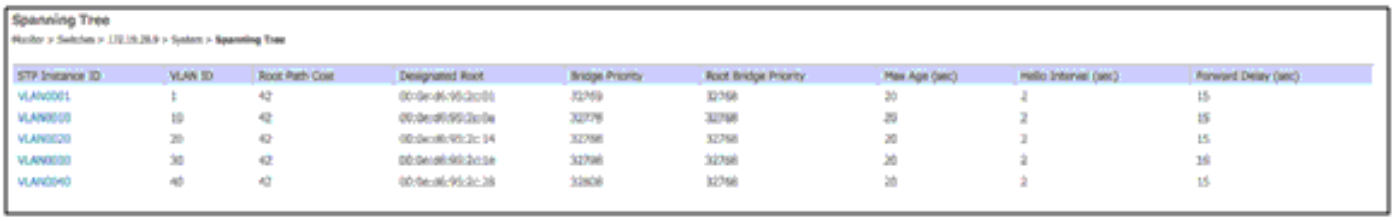


Os clientes prendidos são descobertos através do SNMP traps, do polling snmp e dos mensagens do syslog do Switches.

Com NC, o Switches do Cisco catalyst pode ser monitorado para esta informação:

- Chassi: UDI, nome modelo, uptime
- Utilização Memory/CPU
- Portas/estado das relações
- Camada 2 (VLAN, VTP, medindo - árvore)
- Ambiente: status do fornecimento de energia e fãs
- Memória e arquivos no sistema
- Clientes (prendidos)

Spanning Tree

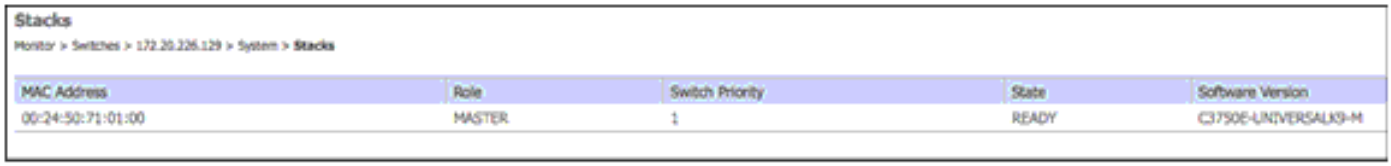


Medida - os detalhes da árvore para cada instância de Spanning Tree são fornecidos:

- Porta STP
- Função da porta
- prioridade da porta
- Custos de caminho
- Estado da porta
- Tipo de porta

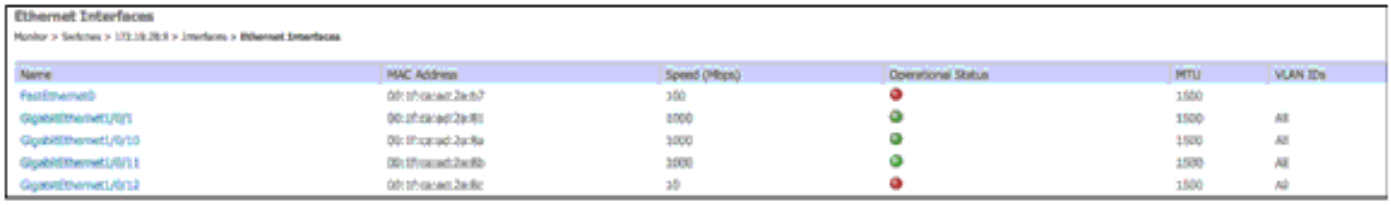
StackWise de Cisco

Para o Switches do Cisco catalyst que apoia a tecnologia da StackWise, cada um comuta o papel na pilha é fornecido que inclui seu papel na pilha, comuta a prioridade, o estado e a versão de software.

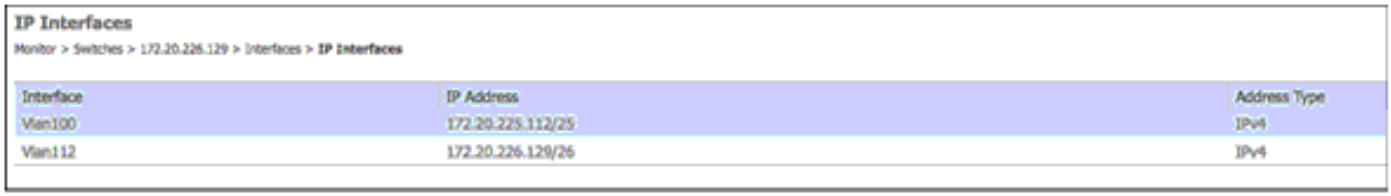


Detalhes da relação

A informação de status em todas as interfaces Ethernet é indicada.

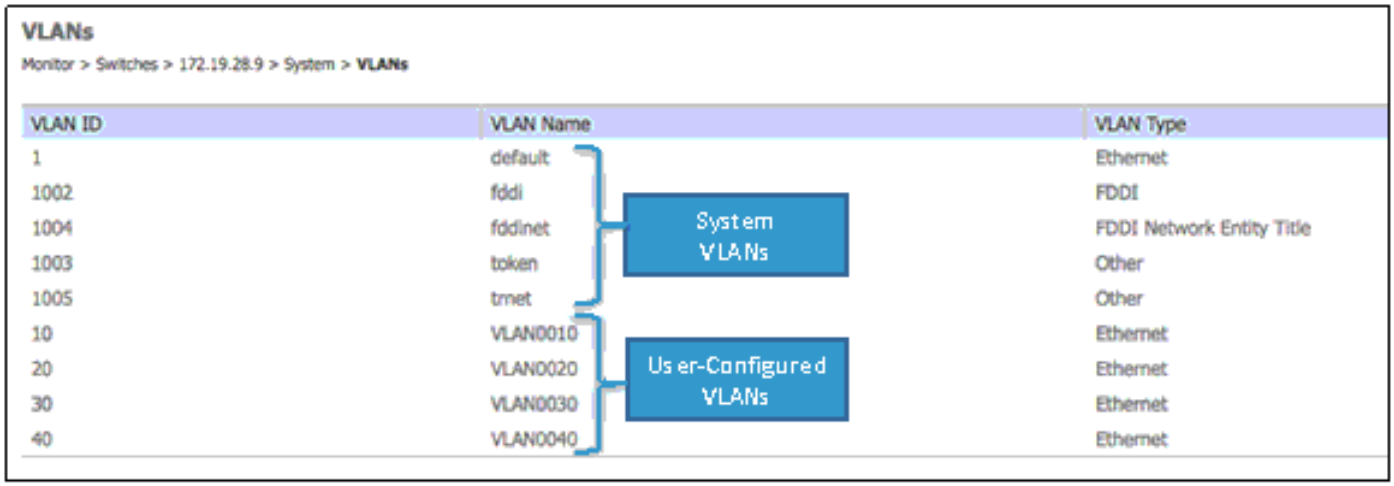


A informação da camada 3 é fornecida igualmente (VLAN ao mapeamento da sub-rede IP).

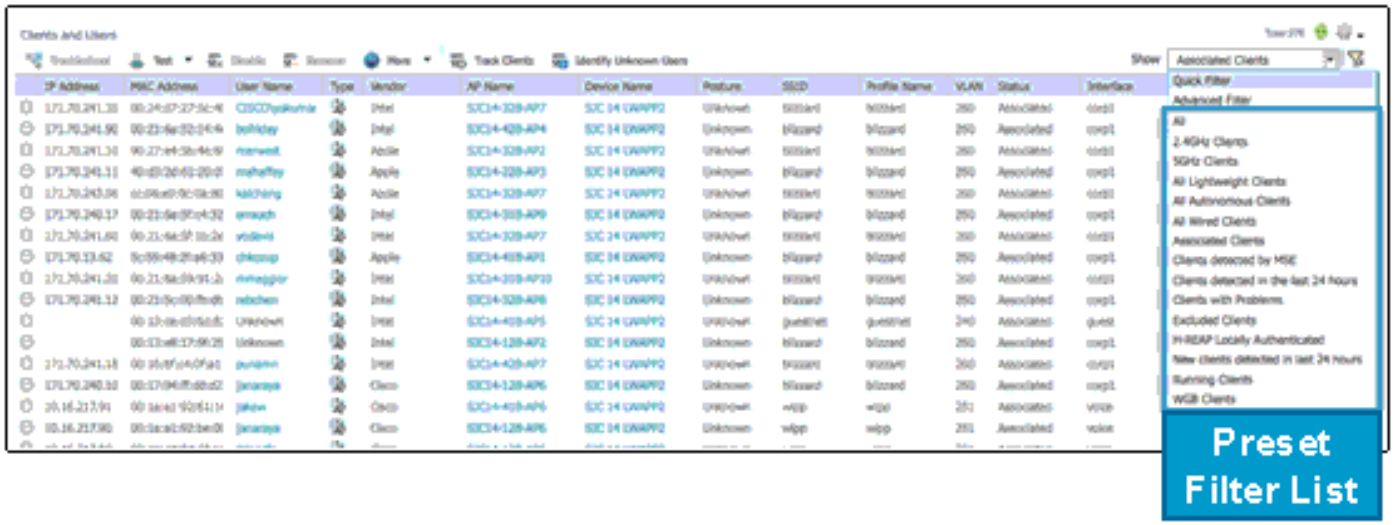


Informação de VLAN

Os detalhes VLAN estão igualmente disponíveis dos NC. O padrão de sistema e o configurado pelo usuário VLAN são indicados. O ID de VLAN, o nome e o tipo são indicados em uma única tela.



Páginas da lista do cliente



Relatórios (Cruz-lançamento e escala)

Os NC 1.0 fornecem o gerenciamento integrado do prendido e dispositivos Wireless/clientes. O SNMP é usado para recolher dados do cliente. O ISE é votado periodicamente para recolher estatísticas do cliente e outros atributos para povoar relatórios relacionados.

Escolha **relatórios > base de lançamento dos relatórios**. Escolha o relatório para a criação/personalização.

Relatórios novos

Conexões superiores N

Isto relata a mostras usuários superiores N em um período de tempo dado baseado nestes medidor:

- Tentativas de conexão
- Tentativas passadas
- Falhas de tentativa

Este relatório contém estas colunas:

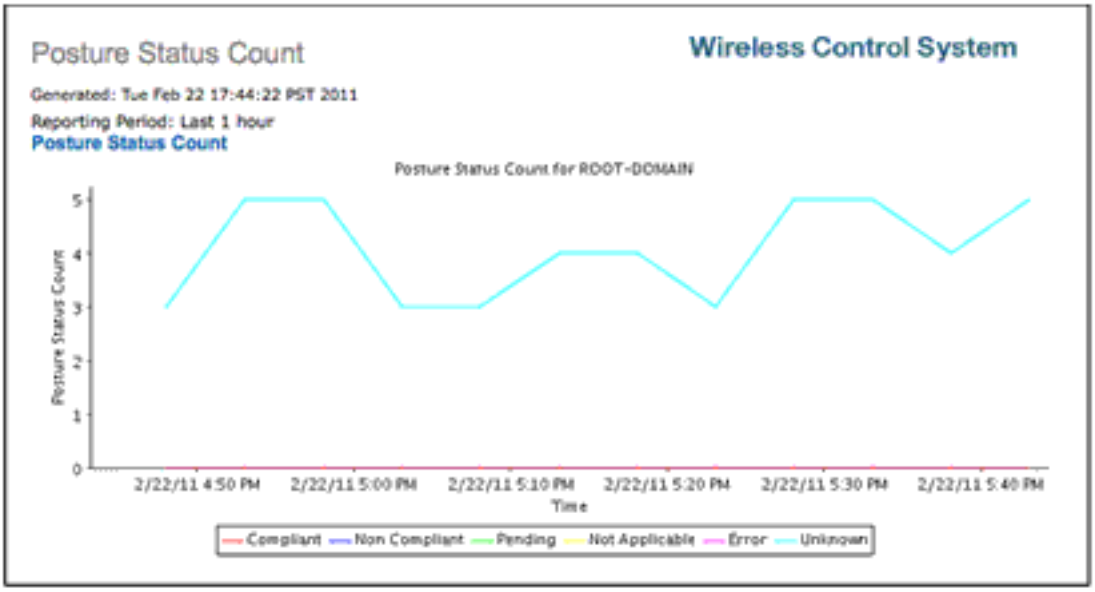
- Username
- Número de tentativas de conexão totais
- Número de tentativas de conexão passadas
- Número de tentativas da falha na conexão

Associação AP

Este as listas de relatório todos os detalhes da associação AP para clientes Wireless e são similares aos relatórios da sessão cliente.

Contagem do estado da postura

Este relatório fornece uma carta da tendência para mostrar ao longo do tempo o estado da postura do cliente. A carta é uma carta de área; a área inferior é o número de clientes passados a verificação da postura e a área superior é o número de clientes que falharam a verificação da postura.



Alarmes/eventos

Os alarmes e os eventos fornecem uma única ideia da página dos alarmes e dos eventos para prendido e Sem fio. O sumário e o navegador persistentes do alarme são indicados no direita inferior da tela apesar de que tela o usuário está. Os NC 1.0 fornecem as opiniões genéricas do alarme que incluem estas páginas:

- Páginas da lista do alarme
- Páginas do detalhe do alarme
- Páginas da lista do evento
- Páginas do detalhe do evento
- Busca do alarme pela categoria & pela categoria secundária
- Janela de sumário do alarme
- Painel do alarme
- Ações do alarme (reconheça, cancele, atribua, unassign, supressão, etc.)
- Notificação de alarme (email, armadilha)

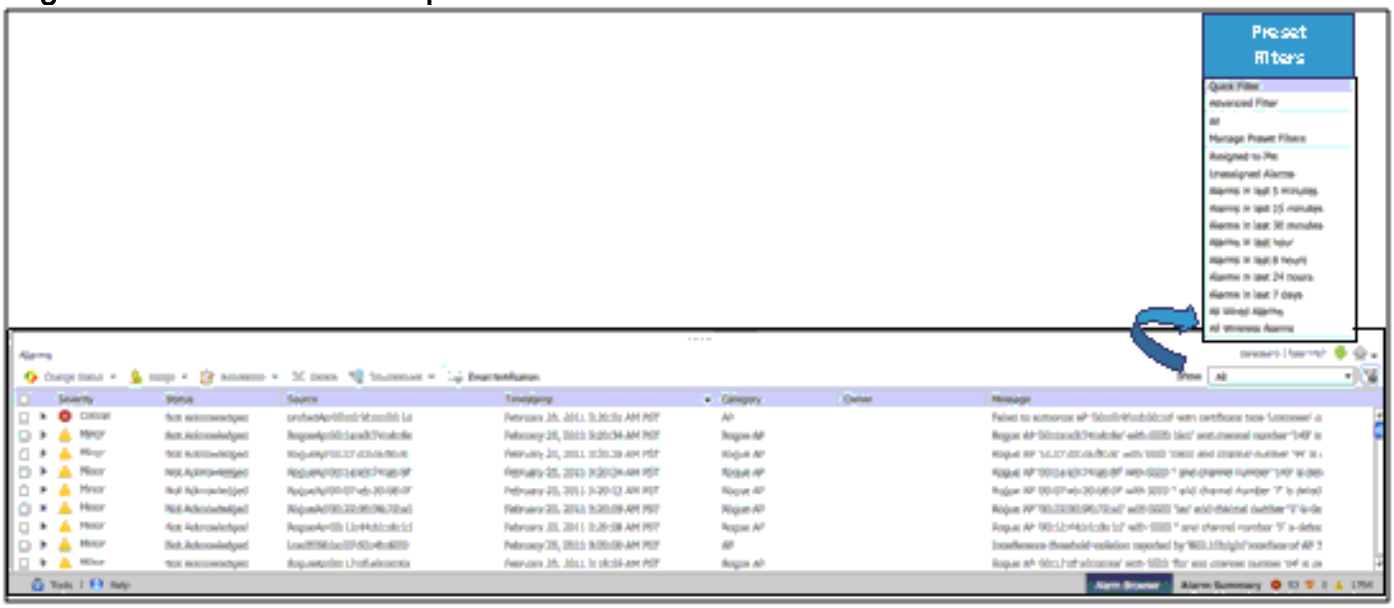
- Navegações da página do alarme (e às vistas diferentes)
- Painel da vista geral do alarme - drilldown à lista filtrada
- Página de Troubleshooting existente do lançamento WCS da página do alarme

As colunas podem ser personalizadas como indicado, hidden, e requisitado novamente. As ações podem ser tomadas em uns ou vários alarmes simultaneamente.

Filtro rápido

Esta característica permite que um usuário filtre em umas ou várias colunas baseadas na sequência de caracteres de texto incorporada ao filtro arquivado na parte superior de cada coluna. Fornece uma ideia filtrada opcional dos alarmes para alarmes prendidos e wireless.

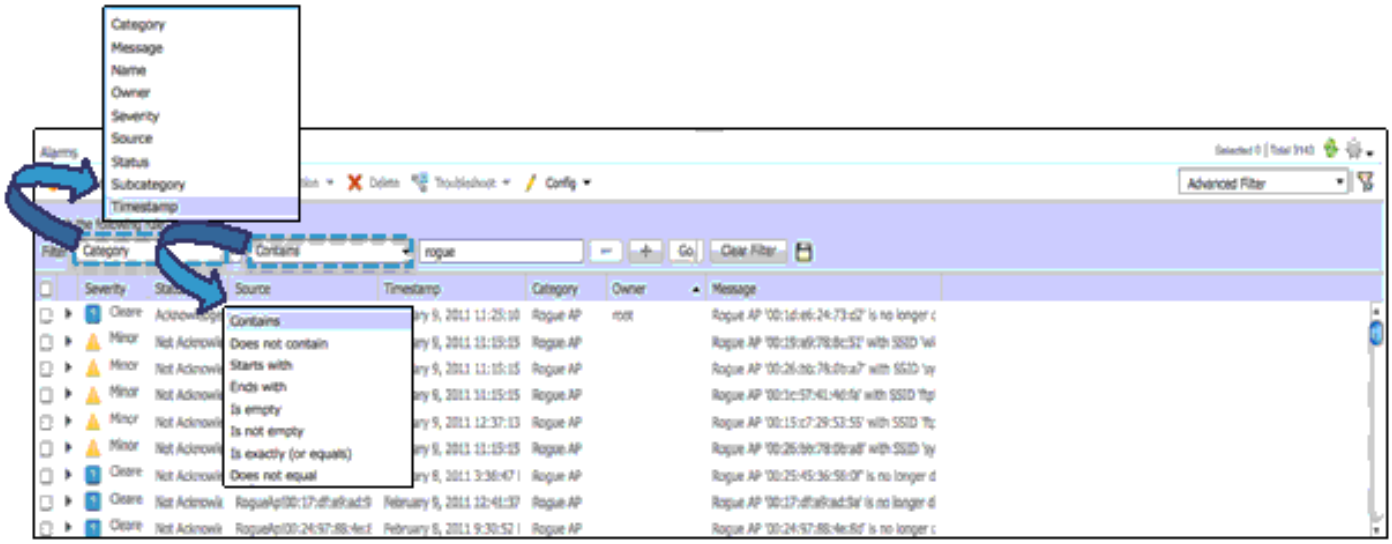
Página dos alarmes – Filtro rápido



Filtro avançado

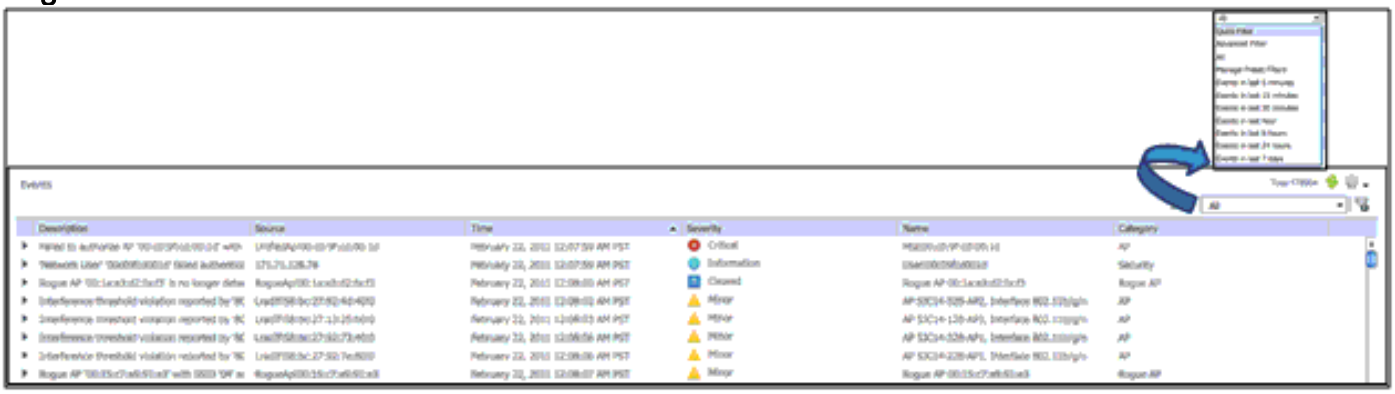
O filtro avançado fornece mesmo a maior capacidade da busca. Fornece a capacidade para procurar em campos específicos com várias condições, como contém, não contém, começa com, e termina com. Este diagrama mostra as várias opções de filtro. Adicionalmente, o filtro avançado permite o aninhamento da circunstância e (E/OU) das circunstâncias booleanas a ser especificadas.

Página dos alarmes – Filtro avançado

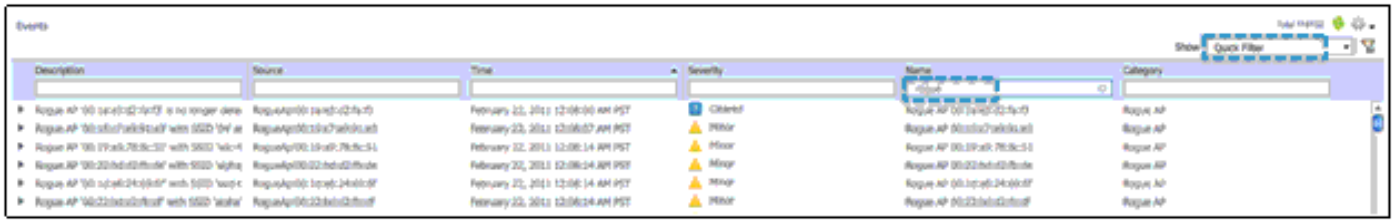


Similarmente, os eventos podem ser indicados e filtro sobre facilmente. Igualmente pré-ajustou, rapidamente e filtros avançados. Estes filtros funcionam de forma similar aos estes o mesmo filtro nos alarmes.

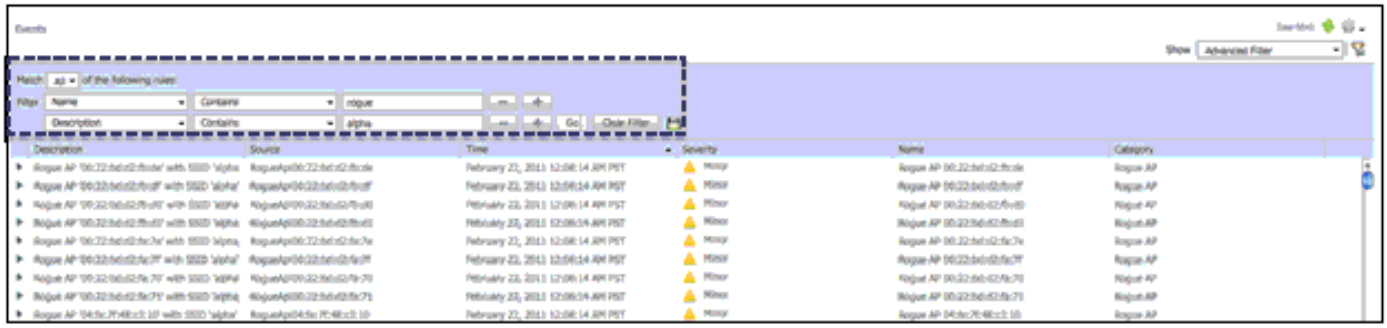
Página dos eventos



Página do evento - Filtro rápido

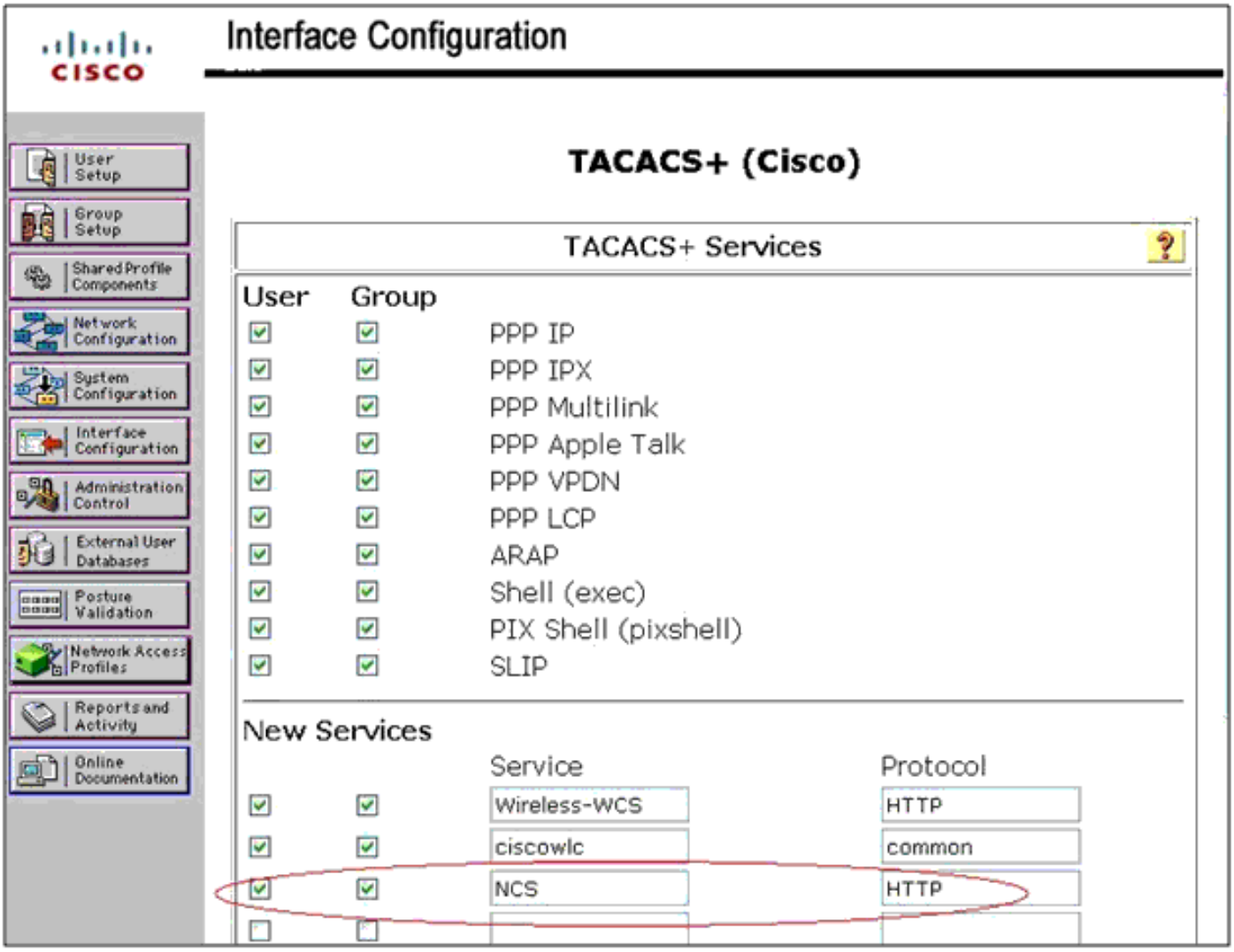


Página do evento - Filtro avançado



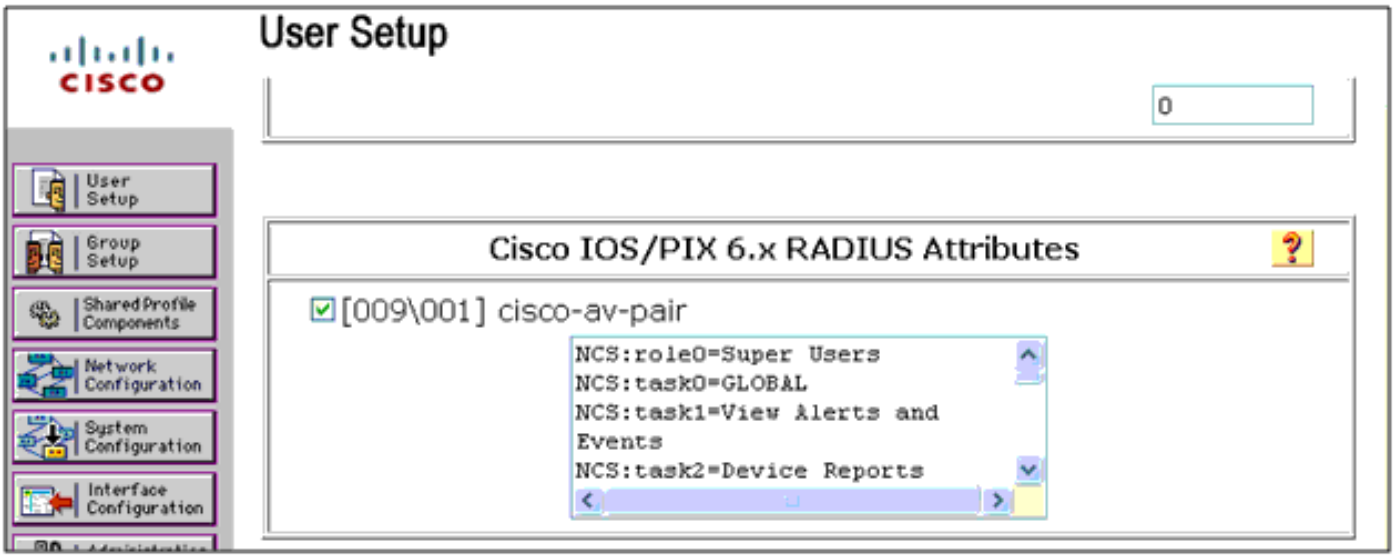
Autenticação de usuário AAA através do TACACS+/RADIUS usando ACS 4.2

Para que os usuários TACACS+ autentiquem com sucesso nos NC, algumas mudanças são exigidas em ACS 4.2. Um serviço novo NC HTTP precisa de ser adicionado na página da configuração da interface para TACACS+ (Cisco IOS).



O grupo inteiro de atributos feitos sob encomenda da lista de tarefas TACACS+ do grupo de usuário NC precisa de ser copiado na área de texto dos atributos feitos sob encomenda NC HTTP segundo as indicações do screen shot para um usuário AAA. O mesmo guarda bom para o grupo de usuário.

Para a autenticação de usuário RADIUS, você precisa de copiar os atributos feitos sob encomenda novos do raio da lista de tarefas do grupo de usuário NC na seção dos atributos RADIUS de Cisco IOS/PIX 6.x para o usuário/grupo de usuário.



Dos NC, adicionar a entrada de servidor nova TACACS+/Radius na **administração > em server AAA > TACACS+/raio**. Ajuste o modo AAA na **administração > em configurações de modo AAA > AAA ao TACACS+/raio** em conformidade. Re-início de uma sessão como o usuário AAA.

Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems