

Considerações e práticas recomendadas para migrar para um sistema de controle de acesso IP





Conteúdo

Sumário executivo	5
Razões para migrar	6
Metas para uma migração	8
Visão geral das considerações	10
Etapas do processo de migração	12
Nossa abordagem à migração	16



Sumário executivo

A migração de um sistema legado de controle de acesso (ACS) para um ACS Protocolo de Internet (IP) torna mais fácil para uma organização operar, expandir e personalizar sua infraestrutura de controle de acesso físico.

Uma migração bem-sucedida ainda requer planejamento e avaliação cuidadosa. Em primeiro lugar, é importante ter um conjunto claro de objetivos. Então, antes de começar a planejar uma migração, uma organização deve avaliar seu sistema existente para determinar os custos e o tempo necessários para concluir o processo.

Por fim, ao lado de um integrador de sistemas, é importante que uma organização siga as etapas principais para realizar uma integração perfeita.

1

Razões para migrar

A migração de um sistema de controle de acesso (ACS) legado centralizado ou distribuído existente para um ACS IP torna mais fácil para uma organização personalizar seu sistema à medida que suas necessidades evoluem, resultando em maior segurança e maior retorno sobre investimento.

Um ACS IP aberto e flexível permite às organizações:

- alavancar a tecnologia IP para padronizar sua infraestrutura de controle de acesso e substituir equipamentos proprietários
- simplificar a futura expansão e modificação da infraestrutura para reduzir o custo total de propriedade (TCO)
- Integrar toda a segurança, controle de acesso e videomonitoramento em uma plataforma unificada com uma única interface
- obter um maior retorno sobre investimento através de utilizações que vão além de bloquear e desbloquear portas

Com uma solução IP, uma organização também pode aproveitar as funcionalidades mais recentes que não estão disponíveis nos sistemas tradicionais. Por esse motivo, é importante considerar como aproveitar os novos recursos ACS oferecidos por soluções IP, incluindo:

- melhorar o gerenciamento e monitoramento multi-site
- escalar para um número maior de portas em uma rede
- aprimorar a cybersecurity com criptografia de ponta a ponta e autenticação avançada
- usar o gerenciamento global de portadores de cartão para mudar para um único cartão em todos os sites

Novas tecnologias ACS ciberneticamente seguras estão disponíveis, o que permite que uma organização aproveite seu sistema para melhorar a segurança e as operações enquanto se protege contra ataques cibernéticos

A manutenção de ACSs físicos tradicionais também está se tornando cada vez mais cara. Quando os componentes legados do ACS atingem o fim de seu serviço, os custos associados à manutenção desses sistemas ou encontrar componentes de reposição aumentam.

Além disso, os ACSs tradicionais carecem da capacidade de resistir a um número crescente de ataques cibernéticos.

Os ACSs legados usam tecnologia desatualizada que os deixa vulneráveis a ameaças cibernéticas. Novas tecnologias ACS de cybersecurity estão disponíveis, o que permite que uma organização aproveite seu sistema para melhorar a segurança e as operações de negócios enquanto se protege contra ataques cibernéticos.

Por fim, como os sistemas legados normalmente operam fornecendo energia separada para cada leitor de cartão e bloqueio, eles são mais caros do que um ACS IP aberto e flexível que suporta PoE para conectar e alimentar todos os controladores de portas, leitores e travas baseados em IP.

2

Metas para uma migração

Depois de decidir migrar de um sistema legado mais antigo para um ACS IP aberto e flexível, uma organização deve considerar os seguintes objetivos ao procurar um provedor de soluções.

2.1 Comprar um sistema com vida útil longa

Ao tentar determinar a vida útil de um ACS, há vários fatores a se considerar:

- **A solução é não proprietária e de arquitetura aberta?**
Uma arquitetura aberta, ACS não proprietário torna mais fácil expandir e modificar o sistema no futuro.
- **O provedor de soluções possui um ecossistema de parceiros desenvolvido?**
A escolha de um provedor de soluções com parceiros de tecnologia em áreas como gerenciamento de ativos, recursos humanos e gerenciamento de visitantes garante maior flexibilidade e mais opções durante a migração e modificações futuras.
- **O provedor de soluções oferece um kit de desenvolvimento de software (SDK) pronto para uso?**
Um SDK pronto para uso permite integração customizada e scripts e possibilita o desenvolvimento de plug-ins para o ACS IP no futuro.

2.2 Reutilizar equipamentos existentes

A migração para um ACS IP aberto e flexível pode aprimorar e proteger o investimento de longo prazo de uma organização em sua infraestrutura de segurança atual, estendendo a vida útil dos componentes existentes e aproveitando novos recursos e aplicações do sistema.

A migração para um ACS IP pode aprimorar e proteger o investimento de longo prazo de uma organização em sua infraestrutura de segurança atual, estendendo a vida útil dos componentes existentes e aproveitando novos recursos e aplicações do sistema.

Além de analisar os recursos, uma organização também deve observar seu fluxo de trabalho de controle de acesso atual para garantir que o provedor de soluções seja capaz de pelo menos manter, se não melhorar, o fluxo de trabalho no novo sistema.

2.3 Trabalho em paralelo

Para realizar uma migração tranquila do ACS, o trabalho de pré-configuração deve ser feito em paralelo e offline para criar a configuração do novo ACS IP no software, incluindo:

- mapeamento do sistema
- importar as entradas e saídas (IOs) dos componentes do sistema
- integrar a lógica para controlar os componentes

2.4 Minimize o tempo de inatividade

Ao migrar um sistema existente, uma organização deve considerar o impacto que o tempo de inatividade terá sobre os usuários do sistema. Durante a fase de escolha é importante determinar:

- as horas de pico durante as quais o ACS deve estar totalmente funcional
- se o novo ACS IP permite ou não a pré-configuração
- se o novo ACS IP pode ser conectado a portas existentes em paralelo

2.5 Certifique-se de que todas as funcionalidades cruciais permanecem disponíveis

É importante que uma organização analise os recursos de hardware e software atualmente usados em seu ACS legado para garantir que esses recursos também estejam disponíveis no novo sistema. Os recursos que devem ser analisados incluem:

- o número de portas que podem ser suportadas
- Gestão de portadores de cartão
- gerenciamento de direitos de acesso
- design de crachá
- necessidades do cliente web
- necessidades de aplicativos móveis
- Gestão de visitantes
- dispositivos de realização de cadastro

Além de analisar os recursos, uma organização também deve observar seu fluxo de trabalho de controle de acesso atual para garantir que o provedor de soluções seja capaz de pelo menos manter, se não melhorar, o fluxo de trabalho no novo sistema.

3

Visão geral das considerações

As considerações a seguir destinam-se a ajudar uma organização a avaliar seu ACS legado atual.

Os resultados dessas avaliações têm impacto direto sobre (1) a decisão de realizar uma migração com substituição total ou parcial, (2) o custo da migração e (3) o tempo necessário para a migração.

3.1 Considerações de hardware

Qualquer migração de um ACS legado para um ACS aberto e flexível IP deve começar avaliando o sistema atual.

A migração para um ACS IP é simplificada se o sistema existente usar cartões e leitores não proprietários. No entanto, se os leitores existentes suportarem comunicação proprietária, provavelmente será necessário uma substituição completa de leitores legados.

Também é importante determinar se os controladores inteligentes existentes e os painéis de interface downstream podem ser reutilizados. Se os controladores existentes forem de arquitetura aberta, existe a possibilidade de incorporá-los ao novo ACS.

3.2 Considerações de software

É importante determinar exatamente o que precisa ser transferido para o novo sistema. Deve-se levar em consideração os dados nativos nas credenciais herdadas, as ferramentas usadas para exportar essas informações do banco de dados atual e quaisquer componentes de terceiros integrados à configuração por meio do SDK.

A migração ACS requer a experiência de engenheiros de pré-vendas, especialistas técnicos, engenheiros de serviço de campo e engenheiros de suporte.

3.3 Considerações de rede

As necessidades de rede do novo sistema IP também devem ser avaliadas ao considerar a migração para uma solução de controle de acesso PoE.

Além disso, uma organização também deve considerar questões de latência e largura de banda em relação à comunicação entre sites ao migrar um sistema distribuído entre sites locais e remotos.

3.4 Considerações de cabeamento

O cabeamento em um ACS legado é outra consideração importante para qualquer migração, pois pode ser possível reutilizar parte do cabeamento existente no novo ACS IP. Antes da migração, é importante comparar as características do cabeamento existente com os requisitos do novo equipamento ACS IP. Além disso, se uma organização deseja expandir seu ACS atual durante a migração, deve-se levar em consideração o cabeamento extra que será necessário.

3.5 Considerações sobre alimentação (energia)

Antes da migração, também deve ser levado em consideração o tipo de alimentação existente no ACS atual, especificamente se o sistema é de 12 V ou 24 V e CC ou CA e se pode fornecer corrente suficiente para os novos componentes de hardware.

3.6 Considerações sobre treinamento

Qualquer migração bem-sucedida para um sistema IP aberto e flexível requer treinamento abrangente sobre como usar o novo software. Portanto, deve-se considerar o tipo de treinamento necessário para os vários usuários do ACS, com base em suas tarefas e nas aplicações aos clientes que usarão com o novo ACS.

3.7 Suporte durante a migração e posterior

Para uma migração bem-sucedida, é importante levar em consideração o nível de suporte fornecido pelo integrador que instala o novo ACS, bem como pelos fabricantes e provedores de soluções cujos componentes irão compor o novo sistema. A migração ACS requer a experiência de engenheiros de pré-vendas, especialistas técnicos, engenheiros de serviços de campo e engenheiros de suporte.

4

Etapas do processo de migração

Há várias etapas envolvidas em uma migração bem-sucedida. Primeiro, o cliente trabalha com um integrador de sistemas e possivelmente com fabricantes e provedores de soluções para elaborar uma cotação e um plano de migração. À medida que o plano está sendo implementado, o suporte técnico e os engenheiros de campo projetarão e configurarão o novo sistema baseado em IP.

4.1 Conheça os fatos

O primeiro passo para o integrador de sistemas é criar a configuração do ACS atual, incluindo detalhes como a localização dos armários elétricos e de telecomunicações, cabeamento e o tipo de energia atualmente usado. Também é importante compilar uma lista completa dos componentes de hardware, servidores e equipamentos de rede usados atualmente no sistema, bem como fornecer detalhes sobre os recursos de software atuais que serão necessários.

4.2 Entenda os requisitos do novo sistema

Para desenvolver um plano de migração bem-sucedido, os seguintes requisitos do novo ACS IP aberto e flexível devem ser reconhecidos e confirmados:

- Componentes de hardware
- Componentes de software
- Configuração de rede
- Cabeamento
- Alimentação (energia)

Entender esses requisitos é fundamental para projetar a arquitetura do novo sistema.

Uma visão completa sobre o ACS atual de uma organização e os requisitos para o novo sistema é essencial para determinar quais componentes de hardware, software, energia, cabeamento e rede podem ser reutilizados.

4.3 Levantamento sobre o local

A próxima etapa é um tour pelas instalações com o cliente, o integrador de sistemas e, possivelmente, com os fabricantes, para garantir que nenhuma parte do sistema existente tenha sido desconsiderada. A pesquisa sobre o local também pode ser a primeira etapa do processo geral. O objetivo da pesquisa sobre o local é:

- obter uma imagem clara da arquitetura e layout do sistema existentes
- determinar onde o equipamento está concentrado
- medir as distâncias entre painéis de controle de acesso, fontes de energia e leitores

4.4 Determinar os componentes que podem ser reutilizados

Uma visão completa sobre o ACS atual de uma organização e os requisitos para o novo sistema é essencial para determinar quais componentes de hardware, software, energia, cabeamento e rede podem ser reutilizados.

4.5 Testando componentes existentes

Depois de determinar quais componentes do sistema existente podem ser reutilizados, os componentes devem ser testados para garantir a compatibilidade.

4.6 Definir novas necessidades de equipamentos

Com uma compreensão clara do que pode ser reutilizado do sistema legado existente e do que é necessário no novo sistema, o integrador deve agora determinar as novas necessidades de rede e controle de acesso.

4.7 Entenda os bancos de dados e também dados existentes

Determinar como importar os dados existentes dos portadores de cartão e da credencial para o novo ACS IP é a próxima etapa do processo de migração. Para aproveitar os dados existentes de software de terceiros, os especialistas técnicos ou engenheiros de campo precisarão exportar os dados dos portadores de cartão e da credencial do sistema existente para um formato de arquivo utilizável.

4.8 Planejar a migração

Para reduzir ao mínimo o tempo de inatividade durante a migração, a migração de hardware deve ser cuidadosamente planejada para garantir que o máximo possível de instalação de software e hardware seja realizado em paralelo.

4.9 Testar o novo sistema IP

Para garantir uma migração tranquila, o integrador deve realizar um passo a passo completo do novo sistema IP antes de efetuar a migração.

4.10 Executar os testes de migração e aceitação

Seguindo o cronograma desenvolvido como parte do plano de migração, o integrador de sistemas e o cliente podem agora iniciar a transição do antigo para o novo ACS. Nesse ponto, é importante deixar os fabricantes de prontidão caso surja algum problema com algum dos novos componentes do ACS.

Para garantir uma migração tranquila, o integrador deve realizar um passo a passo completo do novo sistema IP antes de efetuar a migração.



5

Nossa abordagem para migração

Para garantir uma migração perfeita, a Genetec está disponível durante todo o processo — desde a pesquisa inicial e o planejamento da migração até o teste e suporte do sistema. Em sua função de provedora de soluções, a Genetec oferece aos integradores de sistemas acesso a engenheiros de pré-vendas, de campo e de suporte técnico.

Security Center Synergis™, o sistema de controle de acesso IP da Genetec, oferece aos clientes a vantagem de trabalhar com uma plataforma de arquitetura aberta. Com o Synergis, uma organização tem o poder de atualizar para a tecnologia suportada mais recente a qualquer momento ou até mesmo unificar sua segurança e operações em uma única plataforma. Essa plataforma de arquitetura aberta também oferece aos clientes muito mais flexibilidade em relação a integrações de sistemas de terceiros. A adaptabilidade do Synergis permite que uma organização amplie seu sistema à medida que suas necessidades evoluem, capacitando-as para aumentar a segurança e gerar um maior retorno sobre o investimento.

Procurando por onde começar?

Baixe nossa lista de verificação com as 7 principais coisas a considerar antes de migrar para um sistema de controle de acesso IP.

[Obter minha checklist](#)

Fundada em 1997, a Genetec é líder global em plataformas de segurança unificadas, com uma ampla oferta para uma variedade de especialidades de segurança.

Videomonitoramento: Obtenha uma maior consciência situacional e aumente a segurança em sua cidade com a capacidade de compartilhar câmeras entre agências e organizações, fornecendo uma imagem operacional em comum e melhorando o tempo de resposta a incidentes.

Controle de acesso: Aumente a segurança da sua organização de forma eficaz, responda às ameaças e tome decisões mais claras e em tempo hábil usando uma plataforma unificada e pronta para IP, seja para implantação de um novo sistema de controle de acesso ou para atualizar uma instalação existente.

Reconhecimento automático de placas de veículos: Automatize a detecção de veículos de interesse, aumente a eficiência da fiscalização em estacionamentos e acelere as investigações de segurança pública por meio da capacidade de compartilhar informações de placas de veículos com agências selecionadas e organizações parceiras, sem violar propriedade e privacidade.

Suporte à decisão operacional: Gere mais eficiência no tratamento de incidentes e tomada de decisões através de fluxos de trabalho avançados que guiam os operadores durante alertas de situação por meio de procedimentos baseados em políticas para exportação de compilação detalhada de casos.

Gerenciamento de caso investigativo: Simplifique o gerenciamento de casos e acelere as investigações com uma plataforma que permite centralizar evidências digitais e colaborar de forma segura com investigadores, agências externas e o público.

Serviços na nuvem: Estenda os recursos do seu sistema de segurança on-premises e reduza os custos de TI com serviços na nuvem altamente escalável, on-demand que capacitam sua cidade a lidar facilmente com os requisitos de segurança em rápida mudança e operar com maior eficiência.

Genetec Inc.
genetec.com/locations
info@genetec.com
@genetec

© Genetec Inc., 2023. Genetec e o Logo Genetec são marcas comerciais da Genetec Inc., e podem estar registradas ou pendentes de registro em diversas jurisdições. Outras marcas registradas usadas neste documento podem ser marcas registradas dos fabricantes ou fornecedores dos respectivos produtos.